PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-015147**

(43)Date of publication of application : **18.01.2002**

(51)Int.Cl. **G06F 17/60**
G06F 15/00

(21)Application number : **2000-266072**

(22)Date of filing : **01.09.2000**

(71)Applicant : **MATSUSHITA ELECTRIC IND CO LTD**

(72)Inventor : **TAGAWA KENJI**
HIROTA TERUTO
MATSUSHIMA HIDEKI
INOUE MITSUHIRO
KAMISAKA YASUSHI
HARADA TOSHIHARU
YUGAWA YASUHEI
MIYAZAKI MASAYA
NAKANISHI MASANORI
KOZUKA MASAYUKI

(30)Priority

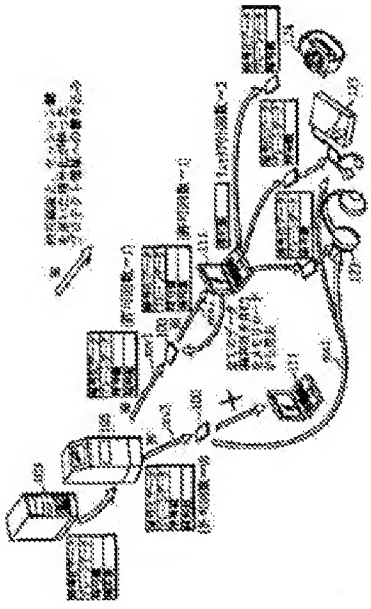
Priority number	Priority date	Priority country
11247922	**01.09.1999**	**JP**
11258582	**13.09.1999**	**JP**
11274182	**28.09.1999**	**JP**
2000125864	**26.04.2000**	**JP**

(54) DISTRIBUTION SYSTEM, SEMICONDUCTOR MEMORY CARD, RECEIVER, COMPUTER READABLE RECORDING MEDIUM AND RECEIVING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a distribution system capable of realizing high convenience when a device manages check-out/check-in.

SOLUTION: A distribution server 103 distributes contents through a network, a KIOSK terminal 105 receives the contents supply through the network and records the contents on an SD memory card 100. A customer's device 111 receives contents supply through the memory card 100, performs check-out of the contents and records a duplicate on a recording medium. SD-AUDIO players 122 to 124 receive contents duplicate supply and reproduces the contents. In such a case, the KIOSK terminal 105 records a usage rule being the registration certificate of right to manage contents recording on the memory card 100 and sets movement control information showing how many times the right movement is approved in the usage rule.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－15147
（P2002－15147A）
(43)公開日　平成14年１月18日(2002.1.18)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	３０２	Ｇ０６Ｆ　17/60	３０２Ｅ	５Ｂ０４９
	ＺＥＣ		ＺＥＣ	５Ｂ０８５
	１４２		１４２	
	５１０		５１０	
	５１２		５１２	

審査請求　有　　請求項の数13　ＯＬ　（全 46 頁）　最終頁に続く

(21)出願番号　特願2000－266072(P2000－266072)

(22)出願日　平成12年９月１日(2000.9.1)

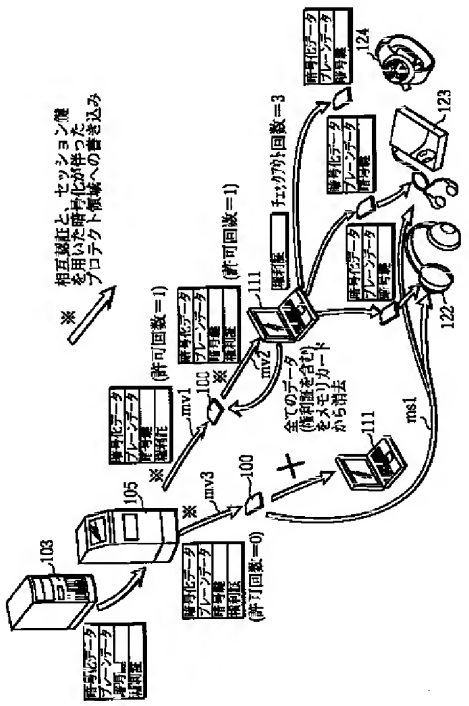
(31)優先権主張番号　特願平11－247922
(32)優先日　平成11年９月１日(1999.9.1)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平11－258582
(32)優先日　平成11年９月13日(1999.9.13)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平11－274182
(32)優先日　平成11年９月28日(1999.9.28)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　田川　健二
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　廣田　照人
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗　（外１名）

最終頁に続く

(54)【発明の名称】　配信システム、半導体メモリカード、受信装置、コンピュータ読取可能な記録媒体、及び受信方法

(57)【要約】
【課題】　機器がチェックアウト チェックインを管理する場合に、高い利便性を実現することができる配信システムを提供する。
【解決手段】　配信サーバ１０３は、コンテンツをネットワークを介して配信し、KIOSK端末１０５は、ネットワークを介した前記コンテンツの供給を受けて、コンテンツをSDメモリカード１００に記録する。カスタマーズデバイス１１１は、SDメモリカード１００を介したコンテンツの供給を受けて、コンテンツのチェックアウトを行い、複製物を記録媒体に記録する。SD-AUDIOプレーヤ１２２～１２４は、コンテンツの複製物の供給を受けて、コンテンツの再生を行う。この際、KIOSK端末１０５は、SDメモリカード１００にコンテンツの記録を管理する権利の権利証であるユーセージルールを記録し、このユーセージルール内に上記権利の移動を何回認めるかを示す移動制御情報を設定する。



【特許請求の範囲】
【請求項１】　コンテンツをネットワークを介して配信する配信サーバと、ネットワークを介してコンテンツを受信する第１、第２受信装置とを含み、受信されたコンテンツの複製物を記録媒体に記録して、再生装置に供給する配信システムであって、
前記第１受信装置は、
コンテンツと、記録媒体に対する当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第１受信手段と、
前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーセージルール情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録手段とを備え、
前記第２受信装置は、
前記データセットをネットワークを介して配信サーバから受信して、保持する第２受信手段と、
前記配布媒体から許可情報を読み出し、読み出された許可情報に、データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内部へのデータセットの移動を行い、データセットを保持するデータセット移動手段と、
第２受信手段及びデータセット移動手段の何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウト手段とを備え、
記録媒体に記録された複製物は、前記再生装置に供給されることを特徴とする配信システム。
【請求項２】　前記配信システムにおいて前記管理情報は、チェックアウトが行なえる残り回数を示し、
前記チェックアウト手段は、前記記録媒体と接続する接続手段を有していて、当該接続手段に接続された記録媒体に未だコンテンツの複製物が記録されておらず、前記第２受信手段、又は、前記データセット移動手段に保持されている管理情報が、1以上の残り回数を示している場合、データセット移動手段が保持しているデータセットにおけるコンテンツの複製物を記録媒体に記録するものであり、
前記第２受信装置は更に
接続手段に接続された記録媒体に既にコンテンツの複製物が記録されている場合、接続手段に接続された記録媒体に記録されているコンテンツの複製物を削除するチェックイン手段と、
記録媒体に複製物が記録されれば、チェックアウトの残り回数をデクリメントするよう第２受信手段又はデータセット移動手段に保持されている管理情報を更新し、記録媒体におけるコンテンツの複製物が削除されればチェックアウトの残り回数をインクリメントするよう管理情報を更新する更新手段とを備えることを特徴とする請求項１記載の配信システム。
【請求項３】　前記記録媒体には、自身に固有の識別子が付与されており、
前記チェックアウト手段は
保持しているコンテンツに、固有の識別子を割り当てて、記録媒体に記録する割当部と、
接続手段に接続された記録媒体に固有な識別子を記録媒体から読み出し、これと、割当部により割り当てられたコンテンツの識別子との組みを記憶する記憶部とを備え、
前記チェックイン手段は
既にコンテンツの複製物が記録されている記録媒体が接続手段に接続されたなら、当該記録媒体に固有な識別子と、コンテンツに固有な識別子との組みを読み取る読取部と、
読取部により読み取られた識別子の組みと、記憶部が記憶している識別子の組みとを比較することにより、接続手段に接続された記録媒体に記録されている複製物が、過去に自装置が記録したものと同一であるか否かを判定する比較部と、
過去に自装置が記録したものと同一である場合、接続手段に接続された記録媒体に記録されている複製物を読み出して保持し、その後、記録媒体から複製物を削除する保持部とを備えることを特徴とする請求項２記載の配信システム。
【請求項４】　請求項３記載の前記データセット移動手段は、
前記配布媒体に記録されている許可情報に、データセットの移動を許可しない旨が示されている場合、コンテンツとユーセージルール情報の移動は行わず、
再生装置は更に、
前記許可情報に移動を許可しない旨が示されている場合、これに対応するコンテンツを直接配布媒体から再生することを特徴とする請求項３記載の配信システム。
【請求項５】　コンテンツをネットワークを介して配信する配信サーバと、ネットワークを介したコンテンツの供給を受けて、コンテンツを配布媒体に記録する第１受信装置と、配布媒体を介したコンテンツの供給を受けて、コンテンツの複製物を記録媒体に記録する第２受信装置と、記録媒体を介したコンテンツの複製物の供給を受けて、コンテンツの再生を行う再生装置とを含む配信システムにおいて、配布媒体として用いられる半導体メモリカードであって、
コンテンツと、ユーセージルール情報とが記録されているボリューム領域を備え、
前記ユーセージルール情報は、記録したコンテンツの記録媒体に対する複製を管理する管理情報と、管理情報及びコンテンツが第２受信装置に移動することを許可する

か否かを示す許可情報とを含むことを特徴とする半導体メモリカード。

【請求項６】　前記コンテンツは、暗号化されたオーディオデータと、暗号化オーディオデータの暗号化に用いられた暗号鍵との組みを含み、

前記ボリューム領域は、

半導体メモリカードと接続している機器の正当性が認証された場合のみ、当該機器によりアクセスされる領域であり、ユーセージルール情報と、暗号鍵とが記録されているプロテクト領域と当該機器の正当性が認証されるか否かに拘らず、当該機器によりアクセスされる領域であり、暗号化オーディオデータが記録されているユーザデータ領域と、

を備えることを特徴とする請求項５記載の半導体メモリカード。

【請求項７】　前記許可情報は、管理情報及びコンテンツの移動が許可されている場合、その許可回数を併せて示すことを特徴とする請求項６記載の半導体メモリカード。

【請求項８】　コンテンツをネットワークを介して配信する配信サーバと、ネットワークを介したコンテンツの供給を受けて、コンテンツを配布媒体に記録する第１受信装置と、配布媒体を介したコンテンツの供給を受けて、コンテンツの複製物を記録媒体に記録する第２受信装置と、記録媒体を介したコンテンツの複製物の供給を受けて、コンテンツの再生を行う再生装置とを含む配信システムにおける第１受信装置であって、

コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第１受信手段と、

前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーセージルール情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録手段とを備えることを特徴とする受信装置。

【請求項９】　ネットワークを介して配信サーバからコンテンツの供給を受けると共に、コンテンツが記録された配布媒体の供給を受けて、コンテンツの複製物を記録媒体に記録する受信装置であって、

前記コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する受信手段と、

前記管理情報と、前記データセットを受信装置に移動することを許可するかを示す許可情報とを含むユーセージルール情報が記録されており、尚且つ、ユーセージルール情報に含まれる許可情報に、前記データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内部へのデータセットの移動を行い、データセットを保持するデータセット移動手段と、

受信手段及びデータセット移動手段の何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウト手段とを備えることを特徴とする受信装置。

【請求項１０】　コンテンツをネットワークを介して配信する配信サーバと、ネットワークを介したコンテンツの供給を受けて、コンテンツを配布媒体に記録する第１受信装置と、配布媒体を介したコンテンツの供給を受けて、コンテンツの複製物を記録媒体に記録する第２受信装置と、記録媒体を介したコンテンツの複製物の供給を受けて、コンテンツの再生を行う再生装置とを含む配信システムにおいて、第１受信装置としての処理をコンピュータに行わせるプログラムをコンピュータ読取可能な形式で記録している記録媒体であって、

コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第１受信ステップと、

前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーセージルール情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録ステップとからなる手順をコンピュータに行わせるプログラムが記録されていることを特徴とするコンピュータ読取可能な記録媒体。

【請求項１１】　ネットワークを介して配信サーバからコンテンツの供給を受けると共に、コンテンツが記録された配布媒体の供給を受けて、コンテンツの複製物を記録媒体に記録する受信処理をコンピュータに行わせるプログラムをコンピュータ読取可能な形式で記録している記録媒体であって、

前記コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する受信ステップと、

前記管理情報と、データセットを受信装置に移動することを許可するか否かを示す許可情報とを含むユーセージルール情報が前記コンテンツと共に前記配布媒体に記録されており、尚且つ、ユーセージルール情報に含まれる許可情報に、前記データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内サブステップへのデータセットの移動を行い、データセットを保持するデータセット移動ステップと、

受信ステップ及びデータセット移動ステップの何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセ

ットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウトステップとからなる手順をコンピュータに行わせるプログラムが記録されていることを特徴とするコンピュータ読み取り可能な記録媒体。
【請求項１２】　コンテンツをネットワークを介して配信する配信サーバと、ネットワークを介したコンテンツの供給を受けて、コンテンツを配布媒体に記録する第１受信装置と、配布媒体を介したコンテンツの供給を受けて、コンテンツの複製物を記録媒体に記録する第２受信装置と、記録媒体を介したコンテンツの複製物の供給を受けて、コンテンツの再生を行う再生装置とを含む配信システムにおいて、第１受信装置に適用される受信方法であって、
コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第１受信ステップと、
前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーセージルール情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録ステップとからなることを特徴とする受信方法。
【請求項１３】　ネットワークを介して配信サーバからコンテンツの供給を受けると共に、コンテンツが記録された配布媒体の供給を受けて、コンテンツの複製物を記録媒体に記録する受信方法であって、
前記コンテンツと、当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する受信ステップと、
前記管理情報と、前記データセットを受信装置に移動することを許可するか否かを示す許可情報とを含むユーセージルール情報が前記コンテンツと共に前記配布媒体に記録されており、尚且つ、ユーセージルール情報に含まれる許可情報に、前記データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内サブステップへのデータセットの移動を行い、データセットを保持するデータセット移動ステップと、
受信ステップ及びデータセット移動ステップの何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウトステップとからなることを特徴とする受信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子音楽配信(Electronic Music Distribution(EMD))等、デジタル著作物の配信サービスを実現する配信システム、半導体メモリカード、受信装置、コンピュータ読取可能な記録媒体、及び受信方法に関する。
【０００２】
【従来の技術】配信システムは、配信サーバと、コンテンツの購入を行う機器と、コンテンツの再生を行う再生装置とからなり、世界にはりめぐらされた各種ネットワークを介して、様々な地域に居住する人々に、著作物を購入する機会を与えるものである。ユーザが所有しているパソコンを購入機器として用いた場合、コンテンツの購入は以下の過程を経て行われる。ユーザがパソコンを操作して、配信サーバーに購入要求を送信したものとする。購入要求が送信されれば、配信サーバは、ユーザに対して課金を行い、その後、デジタル著作物を送信する。ユーザが操作するパソコンは、こうして送信された著作物を受信して、パソコンのハードディスク(以下HDという)に書き込む。著作物の書き込みが正常に行われれば、著作物の購入は完了したこととなる。
【０００３】著作物を購入した機器は、チェックアウト チェックインと呼ばれる処理を実行する。チェックアウトとは、半導体メモリカードやミニディスク等、可搬型記録媒体に著作物(一世代複製物)を記録することをいい、著作物を購入した機器は、3回、4回等、予め決められた回数だけチェックアウトを行うことができる。チェックアウトにより可搬型記録媒体に著作物が記録されれば、上述した再生装置を用いてこの著作物を再生させることができる。しかしチェックアウトが予め決められた回数だけ行われれば、著作物はチェックアウト不可能な状態に設定されることとなる。一方チェックインとは、可搬型記録媒体に記録された著作物(一世代複製物)をパソコンに引き戻す処理であり、チェックアウト不可能な状態に設定された後にチェックインを行えば、再度チェックアウトが可能となる。これらチェックアウト チェックインは、著作権者の利益を不当に害することのないよう、著作権保護を大前提として運営されている。
【０００４】チェックアウト チェックイン時において、著作権がどのように保護されているかを簡単に説明する。ここで複製物を記録すべき記録媒体には、ユーザの通常の操作では読み出せないような領域に固有の識別子（Media-IDと呼ばれる）が記録されており、チェックアウト時には、その記録媒体に固有なMedia-IDを用いて、コンテンツを暗号化する。仮に悪意を持ったユーザが、チェックアウトによりコンテンツが記録された記録媒体から、他の記録媒体へと、コンテンツのコピーを行ったとしても、コピー先の記録媒体に固有なMedia-IDは、コンテンツの暗号化に用いられたMedia-ID（コピー元のMedia-ID）とは異なるので、正常に復号は行えない。この結果著作権は保護されることとなる。
【０００５】ここで現状の配信システムには、ユーザが所有しているパソコンを機器として用いたものの他に、コンビニエンスショップ、レコードショップの店頭や店

内、駅構内に設置されたKIOSK端末を機器として用いたものがある。KIOSK端末を機器に用いた場合、著作物の購入は以下の過程を経て行われる。機器であるKIOSK端末は、ユーザに対して、著作物を記録すべき半導体メモリカードやミニディスク等の可搬型記録媒体を準備させ、この可搬型記録媒体とKIOSK端末とが接続されて、代金が支払れた場合、配信サーバから著作物のダウンロードを行い、可搬型記録媒体に記録する。こうしてKIOSK端末の利用者は、通勤、通学、買い物の途中で、手軽に好みの曲を入手することができる。

【０００６】KIOSK端末により半導体メモリカードに著作物が記録された場合、KIOSK端末以外の機器は、KIOSK端末により半導体メモリカードに記録された著作物をチェックインしようとはしない。その理由は以下の通りである。仮に他の機器がチェックインを行えば、チェックインされた著作物に基づいて、更に3回、4回といったチェックアウトが行われることが考えられる。他の機器へのチェックインと、その機器によるチェックアウトとが繰り返されれば、膨大な数の一世代コピーが行われることとなり、ひいては、著作権保護の形骸化を招いてしまう。こうした一世代コピーの増殖を防止する意味で、他の機器へのチェックインは全面的に禁じられている。

【０００７】

【発明が解決しようとする課題】ところで、KIOSK端末により購入された著作物の他の機器へのチェックインを全面的に禁じるというのは、著作権保護の観点からは合理的であるが、ユーザにとっての利便性は低いと認識されている。即ち、KIOSK端末にて著作物を購入したユーザにとっては、たとえ自宅にパソコン等の機器を所有していたとしても、そのパソコンでチェックアウト チェックインといった機能を享受することができないこととなる。正当な料金を支払ったユーザが、自宅に所有しているパソコンにてチェックアウト チェックインを行えないというのは、ユーザに対する配慮が欠けたものであり、KIOSK端末を利用しようという意欲の消沈を招く恐れが有る。

【０００８】本発明の目的は、著作物を受信した機器がチェックアウト チェックインを管理するという規約が存在する場合に、著作権保護を図りつつも、高い利便性を実現することができる配信システムを提供することである。

【０００９】

【課題を解決するための手段】上述した問題点を解決しつつ上記目的を達成するため、本発明では、著作物の複製物の記録を管理する権利についての権利証であるユーセージルールを”移動”させること提案している。SDMI(Secure Digital Music Initiative)においてこの権利証は、DRMI(Digital Right Management Information)とよばれ、チェックアウトやコピー等を行うにあたっての複製物の世代管理や個数管理は、この権利証に基づいてなされる。この権利証の移動を実現して、上記目的を達成する配信システムは、第１受信装置、第２受信装置を含み、前記第１受信装置は、コンテンツと、記録媒体に対する当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第１受信手段と、前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーセージルール情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録手段とを備え、前記第２受信装置は、前記データセットをネットワークを介して配信サーバから受信して、保持する第２受信手段と、前記配布媒体から許可情報を読み出し、読み出された許可情報に、データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内部へのデータセットの移動を行い、データセットを保持するデータセット移動手段と、第２受信手段及びデータセット移動手段の何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウト手段とを備えることを特徴としている。

【００１０】

【発明の実施の形態】以降、配信システムについての実施形態について説明する。このシステムは、SDMI、SD-Audio Ver1.0規格、SD-Audio Ver1.1規格に準拠して運営されているものとする。SDMI、SD-Audio Ver1.0規格、SD-Audio Ver1.1規格に準拠している機器を対応機器といい、そうでない機器、即ち、SDMI、SD-Audio Ver1.0規格、SD-Audio Ver1.1規格の何れにも準拠していない機器を非対応機器と呼ぶ。SD-AudioVer1.0規格は、曲の特殊再生や編集操作等が可能なように、記録媒体に著作物を記録するための規格であり、SD-Audio Ver1.1規格は、このSD-Audio Ver1.0規格と比べて、著作物の移動や著作物のプレビューを可能とするものである。

【００１１】図１は、著作物のデータ構造を示す図である。本図に示すように著作物は、暗号化データと、暗号化されないプレーンデータと、暗号化に用いられた暗号鍵と、著作物の記録を管理する権利の証明書とから構成される。暗号化データには、MPEG-AACストリームデータ、JPEG静止画データがあり、プレーンデータには、MPEG-AACストリームデータ、JPEG静止画データの再生を制御するナビゲーションデータがある。一方、この権利証は、チェックアウトを何回許可するかを示すチェックアウト許可情報、著作物の移動を何回許可するかの移動許可回数を示す移動制御情報、コピー制御情報を含む。これら著作物を構成するデータセットが記録媒体に記録される際の態様には、図２（ａ）～図２（ｃ）に示す3つの態様がある。

【００１２】図２（ａ）は、暗号鍵、権利証抜きで著作物が記録媒体に記録された態様(1)を示す図である。この態様(1)では暗号鍵が存在しないので、暗号化データを復号することは出来ず、著作物の再生は不可能となる。図２（ｂ）は、権利証抜きで著作物が記録媒体に記録された態様(2)を示す図である。態様(2)では、暗号鍵と暗号化データとの組みは揃っているので、著作物を再生する権利はこの記録媒体上に存在することとなる（著作物の実体的な部分をなす暗号化データ及び暗号鍵の組みを本明細書においてコンテンツという場合もある。また暗号鍵と暗号化データとの組みが記録媒体に記録した状態を”再生権利が記録されている状態”という）。しかし記録を管理する権利証は存在しないので、ここに記録された著作物の暗号鍵及び暗号化データを他の記録媒体に記録することはできない。

【００１３】図２（ｃ）は、権利証を含んだ状態で著作物が記録媒体に記録された態様(3)を示す図である。著作物の記録を管理する権利は、この記録媒体を内蔵又は接続している機器に存在することとなる。態様(3)では、著作物の再生のみならず、チェックアウト チェックイン等により図２（ｂ）に示す状態を他の記録媒体に作り出すことも可能となる。

【００１４】続いて、著作物をセキュアに格納することができる配布媒体について説明する。そうした配布媒体の一例として、本実施形態では半導体メモリカード（以下、Secure Digital(SD)メモリカードと称する）を用いるものとする。本図におけるSDメモリカード１００は図３（ａ）に示すような外観形状を有し、長さ32.0 mm、幅24.0 mm、厚さ2.1 mmといった大きさ（切手サイズの大きさ）なので、ユーザはこのSDメモリカード１００を指先で把持することができる。SDメモリカード１００には、機器との接続のための９本のコネクタが設けられており、側面には、記憶内容の上書きを許可するか禁止するかを操作者が設定することができるプロテクトスイッチ１０１が設けられている。

【００１５】図３（ｂ）は、SDメモリカード１００の階層構造を示す図である。本図に示すように、SDメモリカード１００の階層構造は、著作物を構成するデータセットをセキュアに格納するよう構成された物理層、FAT（FAT:File Allocation Table,ISO/IEC 9293）に基づき、クラスタを最小単位としてアクセスされるファイルシステム層、著作物を構成する暗号化データ、暗号鍵、プレーンデータ、権利証が格納される応用層からなる。

【００１６】図３（ｃ）は、SDメモリカード１００における物理層の構成を示す図である。本図に示すように、SDメモリカード１００の物理層は、システム領域１、Hidden領域２、プロテクト領域３、AKE処理部４、AKE処理部５、Ks復号化部６、Ks暗号化部７、ユーザデータ領域８からなる。システム領域１は、Media Key Block(MKB)と、Media-IDとを格納した読出専用領域であり、ここに格納されたMKB、Media-IDを書き換えることはできない。SDメモリカード１００が他の機器と接続され、MKBとMedia-IDとが他の機器により読み出された場合、これらを読み出した他の機器が、MKB、Media-IDと、自身が所持しているデバイス鍵Kdとを用いて所定の演算を正しく行えば、他の機器は正しい暗号鍵Kmuを所持することができる。

【００１７】Hidden領域２は、正解値となる暗号鍵Kmu、即ち、他の機器が正常なデバイス鍵Kdを用いて正常な演算を行なった場合、得られるべき暗号鍵Kmuを格納している領域である。プロテクト領域３は、暗号鍵及び権利証を格納している。Authentication and Key Exchange(AKE)処理部４、AKE処理部５は、機器とSDメモリカード１００との間でチャレンジ レスポンス型の相互認証を行って、相手側の正当性を認証し、相手側が不当であれば処理を中断するが、相手側が正当であれば機器とSDメモリカード１００との間で暗号鍵（セッション鍵Ks）を共有する。機器による認証は3つのフェーズ（機器側で乱数を発生させ、得られた乱数をKmuを用いて暗号化して、チャレンジ値AとしてSDメモリカード１００に送信するChallenge1フェーズ、SDメモリカード１００側でこのチャレンジ値AをSDメモリカード１００内のKmuを用いて復号化し、得られた値をレスポンス値Bとして機器に送信するResponse1フェーズ、機器側で保持していたチャレンジ値Aを機器側のKmuで復号化して、SDメモリカード１００から送信されたレスポンス値Bと比較するVerify1フェーズ）からなる。

【００１８】SDメモリカード１００による認証は3つのフェーズ(SDメモリカード１００で乱数を発生させ、得られた乱数をKmuを用いて暗号化して、この値をチャレンジ値Cとして機器に送信するChallenge2フェーズ、機器側においてこのチャレンジ値Cを機器内のKmuを用いて復号化し、得られた値をレスポンス値DとしてSDメモリカード１００に送信するResponse2フェーズ、SDメモリカード１００側で保持していたチャレンジ値CをSDメモリカード１００側のKmuで復号化して、機器から送信されたレスポンス値Dと比較するVerify2フェーズ）からなる。

【００１９】この際、他の機器が不正な暗号鍵Kmuを用いて相互認証を行えば、フェーズVerify1,2において、チャレンジ値Aとレスポンス値Bとの不一致、チャレンジ値Cとレスポンス値Dとの不一致が判定され、相互認証が中断することとなる。逆に相手側の正当性が認証されれば、AKE処理部４、AKE処理部５は、上述したチャレンジ値Aと、チャレンジ値Cとの排他的論理和をとり、これをKmuにて暗号化することにより、セッション鍵Ksを得る。

【００２０】Ks復号化部６は、SDメモリカード１００と接続された他の機器から、プロテクト領域に書き込むべき暗号鍵、権利証であって、暗号化されたものが出力さ

れた場合、それら暗号鍵、権利証がセッション鍵Ksを用いて暗号化されているものとして、セッション鍵Ksを用いることにより復号を行う。そうして復号により得られた暗号鍵、権利証が本来の暗号鍵、権利証であるとして、プロテクト領域に書き込む。

【００２１】Ks暗号化部７は、SDメモリカード１００と接続された他の機器から、暗号鍵、権利証を読み出す旨のコマンドが出力されると、セッション鍵Ksを用いてプロテクト領域に格納されている暗号鍵、権利証を暗号化した後に、そのコマンドを発行した他の機器に出力する。ユーザデータ領域８は、機器の正当性が認証されるか否かに拘らず、当該機器によりアクセスされる領域であり、暗号化データ、プレーンデータが格納される。プロテクト領域から読み出された暗号鍵が正しい値であれば、ここに格納されている暗号化データは正しく復号されることとなる。プロテクト領域に対するデータ読み書きには、Ks復号化部６による復号化と、Ks暗号化部７による暗号化とが伴うので、プロテクト領域は、SDメモリカード１００と接続している機器がAKEプロセスを正しく行った場合のみ、当該機器により正規にアクセスされることとなる。

【００２２】こうした著作物を構成するデータセットが配置されたSDメモリカード１００に、他の機器が接続された場合、他の機器はどのようなデータを取得することができるかについて説明する。図４（ａ）は1つ目のケースであり、プロテクト領域に暗号鍵のみが格納された状態で非対応機器がSDメモリカード１００に接続された場合を表している。このケースでは、ユーザデータ領域に格納されている暗号化データ、プレーンデータを読み出すことができるが、プロテクト領域にアクセスすることができないため、暗号鍵を取得することはできない。この状態は態様(1)と同様であり、この機器は、SDメモリカード１００と接続しながらも、再生権利を所持できないので著作物を一切再生することができない。

【００２３】図４（ｂ）は2つ目のケースであり、プロテクト領域に暗号鍵のみが格納された状態で対応機器がSDメモリカード１００と接続された場合を表している。この機器はプロテクト領域に格納されている暗号鍵を、ユーザデータ領域に格納されている暗号化データ、プレーンデータと共に読み出すことができる。こうして、暗号化データ、プレーンデータ、暗号鍵を揃えることができるので、この対応機器は、再生権利を所持することができ、著作物を再生させることができる。しかし、プロテクト領域には、権利証が存在せず、この機器は、権利証を読み出すことができないので、この著作物の記録を管理する権利を掌握することはない。

【００２４】図４（ｃ）は3つ目のケースであり、プロテクト領域に権利証及び暗号鍵が格納された状態で対応機器が接続され、権利証が、移動を1回許可する旨を示す移動制御情報を含んでいる場合を表している。プロテクト領域に含まれる権利証が、1回の移動を許可する旨の移動制御情報を含んでいるので、機器は、権利証ごと著作物をSDメモリカード１００から読み出し、自身が内蔵している記録媒体に格納しておくことができる。機器が権利証を内蔵記録媒体に記録した状態では、内蔵記録媒体とSDメモリカード１００とに著作物が存在しており、また権利が二重に発生していることとなるので、機器は著作物を、SDメモリカード１００から消去するという処理を行う。こうした削除により、機器は、管理権と共に著作物をSDメモリカード１００から譲り受けたこととなる。

【００２５】図４（ｄ）は4つ目のケースであり、プロテクト領域に権利証及び暗号鍵が格納された状態で対応機器が接続され、権利証に含まれる移動許可回数が0回の場合を示す図である。移動制御情報に示される移動の許可回数が0回なので、権利証を移動させることができず、管理権を掌握することはできない。この場合、著作物は、SDメモリカード１００において著作物の”原盤”のように扱われることとなる。許可回数が”0”となるケースは、元々、移動許可回数は1以上の値であったが、機器の移動が何度か行われ、移動許可回数のデクリメントが繰り返たため、”0”になった場合に生じる。

【００２６】以上でSDメモリカード１００の構成についての説明を終える。続いて、EMDにおける機器について説明する。EMDにおける機器には、配信サーバー、デジタルターミナル（第１受信装置）、カスタマーズデバイス（第２受信装置）、SD-AUDIOプレーヤ１２２～１２４（再生装置）といった4つの種別があり、以降これらを順に説明する。本実施形態に係る配信サーバー及びデジタルターミナルのうち代表的なものを図５～図６（ｂ）に示し、本実施形態におけるカスタマーズデバイスのうち、代表的なものを図７（ａ）、再生装置のうち、代表的なものを図７（ｂ）に示す。

【００２７】図５における配信サーバー１０３は、複数の著作物を構成するデータセットを記憶しており、それらのうち、何れかのものの購入がデジタルターミナルやカスタマーズデバイスから申し出されると、購入の申出があった著作物をネットワークを介して、デジタルターミナルやカスタマーズデバイスに送信する。図５、図６（ａ）、図６（ｂ）におけるデジタルターミナル１０４～１１０は、対応機器の1つであり、ネットワークを介して音楽会社が運営している配信サーバー１０３から著作物を構成するデータセットを譲り受け、SDメモリカード１００に記録する。ここでネットワークには、ISDN、PSTN等の有線ネットワーク、衛星放送回線、セルラーシステム等、様々な形態の無線ネットワークを含み、デジタルターミナル１０４～１１０には、駅や空港の構内や、レコードショップ、コンビニエンスショップの店頭に設置されたKIOSK端末１０４～１０８、無線セルラーシステムにて通信を行う携帯電話機１０９、衛星放送受

信用のSTB１１０等の種別がある。図５は、駅構内、店頭にKIOSK端末１０４～１０８が設置されている様子を示す図である。図６（ａ）は、携帯電話機タイプのデジタルターミナル１０９により、著作物を構成するデータセットがSDメモリカード１００に書き込まれる様子を示す図であり、図６（ｂ）は、STBタイプのデジタルターミナル１１０により、著作物を構成するデータセットがSDメモリカード１００に書き込まれる様子を示す図である。KIOSK端末１０４～１０８は、専用の光ファイバー回線を介して配信サーバー１０３と接続されており、上述したデータセットの譲り受けをこの専用回線を介して行う。携帯電話機１０９は、セルラーシステムに設置された無線基地局、交換局を介して上述したデータセットの譲り受けを行い、STB１１０は、通信衛星や専用の光ファイバー回線を介して、データセットの譲り受けを行う。

【００２８】これらの図におけるデジタルターミナルは、配信サーバー１０３をアクセスすることにより、配信サーバー１０３内の記録媒体に格納されている複数の著作物を操作者に提示し、何れかの著作物の購入指示を操作者から受け付ける。操作者が何れかの著作物の購入を行う旨の操作を行えば、その著作物を構成するデータセットの送信を要求する旨の要求信号を配信サーバー１０３に送信する。配信サーバー１０３から、著作物を構成するデータセットが送信されれば、デジタルターミナルはそれらを受信して保持し、その後、これらをSDメモリカード１００に記録する。

【００２９】カスタマーズデバイス１１１～１２１は、ローカルストレージと呼ばれる記録媒体を内蔵して、ネットワークルート、SDメモリカードルート（SDメモリカード１００を介した著作物の取得ルート）で取得した著作物からなるホームライブラリィの管理を行い、SDメモリカード１００又はローカルストレージに記録された著作物の再生やチェックアウトを行う。図７（ａ）は、様々なタイプのカスタマーズデバイスを示す図であり、図７（ｂ）は、様々なタイプのSD-AUDIOプレーヤを示す図である。本図において、カスタマーズデバイスは、パソコンタイプのもの（１１１～１１６）、民生音響機器タイプのもの（１１７～１２１）等様々なタイプがあるが、ローカルストレージを内蔵し、ホームライブラリィの管理という点で共通している。ローカルストレージとは、プロテクト領域と、ユーザデータ領域を含み、図４に示したような態様で、著作物を構成するデータセットをセキュアに格納することができる記録媒体である。以降、パソコンタイプのものを一例にして、カスタマーズデバイスの機能について説明する。

【００３０】先ず初めにネットワークルートにて、カスタマーズデバイスがどのように著作物を取得するかについて説明する。図８（ａ）は、ネットワークに接続された配信サーバー１０３と、複数のユーザが所有するカスタマーズデバイス（パソコン１１１～１１６）とを示す図である。カスタマーズデバイス１１１は、デジタルターミナル同様、ネットワークを介して配信サーバー１０３をアクセスし、複数の著作物のうち、何れかのものを取得してローカルストレージに蓄積する。

【００３１】ネットワークルートで著作物の構築を繰り返すことにより、ローカルストレージにホームライブラリィを構築することができ、著作物の権利証に基づいて、各著作物のチェックアウト チェックインを管理する。図８（ｂ）、図８（ｃ）は、3回という範囲でカスタマーズデバイス１１１がチェックアウト チェックインを行う様子を示す図である。即ち、権利証にチェックアウトが可能な旨が示されており、その上限数が設定されているなら、その上限数の範囲内で、チェックアウトを行う。この際の動作は以下の通りである。カスタマーズデバイス１１１にSDメモリカード１００が接続され、チェックアウトを行う旨が指示されれば、SDメモリカード１００のプロテクト領域に、暗号化データと、プレーンデータとを書き込む。また、プロテクト領域には、著作物における暗号鍵を書き込む。その後Check-Out回数をデクリメントする。3つのSDメモリカード１００に著作物を構成するデータセットが記録され、デクリメントによりCheck-Out回数が"0"になると、カスタマーズデバイス１１１は、図８（ｃ）に示すように、ローカルストレージに格納されている暗号鍵、プレーンデータ、暗号化データをチェックアウト不可能な状態に設定する。

【００３２】この際、チェックアウトによりSDメモリカード１００に著作物を構成するデータセットが記録されたので、対応機器は、SDメモリカード１００と接続することにより、著作物を再生することができるが、それらを別の記録媒体にコピーすることはない。何故なら、対応機器は、権利証を有していないSDメモリカード１００からは、暗号鍵を読み出して、自分の記録媒体や、他の記録媒体に記録するという動作は行わないからである。仮に非対応機器がかかる読み出し及び記録を行おうとしても、そうした非対応機器はプロテクト領域をアクセスすることができず（図４（ａ）参照）、暗号鍵及び権利証の入手には、失敗するので、実質、SDメモリカード１００に記録された権利証抜きの著作物が他の記録媒体に記録されることはない。以上のことから、カスタマーズデバイスからSDメモリカード１００への一世代コピーは認められるが、カスタマーズデバイスにより著作物が記録されたSDメモリカード１００から他の記録媒体への二世代コピーは禁止されることとなる。二世代コピー以降を禁ずることにより、コピーが無尽蔵に行われるのを禁じている。

【００３３】続いてSDメモリカードルートにて、カスタマーズデバイスがどのように著作物を取得するかについて説明する。図９は、本実施形態に係るトラック配信システムに含まれる配信サーバと、複数の機器と、再生装

置とを示す図であり、SDメモリカードルートにて、カスタマーズデバイス１１１が著作物を取得する様子を表している。SDメモリカード１００における著作物の取得処理は以下の通りである。矢印mv1に示すように、SDメモリカード１００に記録されている著作物の権利証が移動を1回以上許可する旨の移動制御情報を含んでいる場合、カスタマーズデバイス１１１は、矢印mv2に示すようにSDメモリカード１００から著作物を構成するデータセットを読み出して、内蔵しているローカルストレージに記録する。その後、著作物を構成するデータセットをSDメモリカード１００から削除する。SDメモリカード１００からの取り込みと、著作物の削除とを行うことにより、ネットワークルートで著作物を取得したのと同じ状況をカスタマーズデバイス内に作り出すことができ、以降、カスタマーズデバイスは権利証に従って、チェックアウトを行うことができる。一方、矢印mv3に示すように、SDメモリカード１００に記録されている著作物の権利証が、移動を0回許可する旨の移動制御情報を含んでいる場合、カスタマーズデバイス１１１は、SDメモリカード１００から著作物を構成するデータセットを読み出すということは行わない。矢印ms1に示すように、カスタマーズデバイスを介することなく、このSDメモリカード１００は直接SD-AUDIOプレーヤ１２２、SD-AUDIOプレーヤ１２３、SD-AUDIOプレーヤ１２４に装填され、再生されることとなる。こうやって著作物の権利証を移動させない場合は、著作物の販売価格を安くしてもよい。

【００３４】図９において配信サーバー１０３により”移動許可回数=1回”と移動制御情報が設定された場合には、移動制御情報に示される移動許可回数は以下のように更新されながら、権利証は各記録媒体間を移動してゆくこととなる。

ネットワーク　－－－ -＞ SDメモリカード
”許可回数=1回”　　”許可回数 :0回”

また配信サーバー１０３により”移動許可回数=2回”と設定された場合には、移動制御情報に示される移動許可回数は以下のように更新されながら、権利証は各記録媒体間を移動してゆくこととなる。

【００３５】

ネットワーク　－－－＞ SDメモリカード－－ -＞ ローカルストレージ
”許可回数 :2回”　　”許可回数=1回”　　”許可回数=0回”

更に配信サーバー１０３により”移動許可回数=2回”と設定された権利証をネットワークルートで、カスタマーズデバイスが取得した場合には、移動制御情報に示される移動許可回数は以下のように更新されながら、権利証は各記録媒体（SDメモリカード１００、ローカルストレージ）間を移動してゆくこととなる。

【００３６】

ネットワーク　－－－＞ ローカルストレージ - －－＞SDメモリカード
”許可回数 :2回”　　”許可回数=1回”　　”許可回数=0回”

これからもわかるように、権利証をネットワークルートで取得する場合、移動許可回数が3回に設定されていれば、カスタマーズデバイスから他のローカルストレージへの権利証の移動が可能となる。SDメモリカード１００を介した著作物の移動は可能であるが、ローカルストレージからローカルストレージへの直接移動は、認められないことは注意すべきである。

ネットワーク －－－＞ ローカルストレージ －－
”許可回数=3回”　　”許可回数=2回”

－－ -＞SDメモリカード －－－＞ ローカルストレージ
”許可回数=1回”　　”許可回数=0回”

SD-AUDIOプレーヤ１２２～１２４は、カスタマーズデバイスがチェックアウトを行うことにより可搬型記録媒体に記録された暗号化データを再生する。SD-AUDIOプレーヤ１２２はヘッドフォンタイプ、SD-AUDIOプレーヤ１２３は携帯機器タイプ、SD-AUDIOプレーヤ１２４はリストバンドタイプであり、ユーザは、通勤や通学の途中で、これらに記録された暗号化データを再生させることができる。図９の一例において、カスタマーズデバイス１１１に、著作物を構成するデータセットが移動すれば、カスタマーズデバイス１１１は、権利証に記載に基づいて、例えば3つの可搬型記録媒体に、暗号化データ及び暗号鍵をチェックアウトする。このように3つの可搬型記録媒体に暗号化データ及び暗号鍵がチェックアウトされれば、SD-AUDIOプレーヤ１２２～１２４は、これらを再生させることができる。

【００３７】以上でEMDにおける機器についての説明を終える。続いて、著作物を構成するデータセットの詳細について説明する。先ず初めに配信サーバー１０３からデジタルターミナルへと著作物が伝送される際、著作物はどのようなフォーマットで伝送されるか、即ち、流通時における著作物のデータ構造について説明する。流通時において、曲のような単体の著作物は、パッケージという単位で指示され、また音楽アルバムのような著作物の集合体は、タイトルという単位で指示される。タイトル及びパッケージのデータ構造を示したのが図１０であり、以降、タイトル及びパッケージのデータ構造を図１

０を参照しながら説明する。本図において、タイトルは、1つ以上のパッケージ#1,#2　　#Nからなる。各パッケージは、配信可能なファイルであり、1つのヘッダ、Navigation Structure、複数のContent ELement(CEL#1,#2,#3　　)、Default Offerを含む。

【００３８】『Navigation Structure』は、各CELをどのように再生させるかという再生制御手順を示したデータである。例えば、図１０の一例では、CEL#1の再生時にCEL#3の静止画（ピクチャオブジェクト）を表示する旨がこのNavigation Structureに示されることとなる。『CEL』は、メディア毎に分類された著作物を構成する情報要素である。著作物は曲であるので、著作物は、その曲についての音声と、曲を再生する際、共に表示すべきプロモーション画像等からなり、パッケージは、これらをメディア毎のCELとして格納する。図１０の三段目は、CELの一例を示す。CEL#1は、ある曲の音声をエンコードすることにより得られたMPEG-AACストリームデータであり、CEL#2は、CEL#1であるMPEG-AACストリームデータを2秒間隔で頭出ししてゆく際のデータ間隔を示すタイムサーチテーブル、CEL#3は、CEL#1を再生する際、バックグラウンド映像として表示すべきJPEG静止画データである。このように、ある曲についてのメディア毎の情報は、個々のCELとしてパッケージ内に格納されていることがわかる。これらのうち、AACストリームデータ、静止画データは、著作権保護の観点から暗号化され、暗号化データとしてパッケージ内に収録される。

【００３９】『Default Offer』は、著作物を販売する際に適用すべき商業的な取り決めを示す情報であり、その販売にあたって購入に対する課金額や著作物に含まれる暗号化データを復号するための暗号鍵等を含む。図１１は、Default Offerのデータ構造を階層的に示す図である。本図においてDefault Offerは、『Offer Header』と、『CEL Keychain』と、この著作物の記録を管理する権利についての権利証である『Digital Right Management(DRM)』とを含む。CEL Keychainの内部構成を、破線の引き出し線Df1に引き出して示す。この引き出し線Df1によれば、CEL Keychainは、CEL Keychainについてのヘッダ(CEL Keychain Header(CKH))と、CEL Keychainについての属性を示すCK_ATRと、同じパッケージに含まれるCELを復号するための暗号鍵であるCEL Key(CK)#1,#2,#3,#4　　#nとからなる。

【００４０】DRMの内部構成を、破線の引き出し線Df2に引き出して示す。DRMは、本著作物をSDメモリカード１００に記録した際、SDメモリカード１００からローカルストレージへの移動を許可するか、許可しないかを示す『Move Control Information(MVCNTI)』、著作物がローカルストレージに移動した際、このカスタマーズデバイスのチェックアウトを何回許可するかを示す『Check-Out Control Information(COCNTI)』と、この著作物の再生をどのような条件で許可するかを示す『Permitted Playback Count(PB_COUNT)』と、コンテンツ配信業者のIDが記述される『PPDRM_FR_ID1～4』とからなる。

【００４１】MVCNTIの詳細設定を破線py1にて引き出して示す。00hに設定された際、SDメモリカード１００からローカルストレージへの移動は許可されていない旨を示し、01hに設定された際、SDメモリカード１００からローカルストレージへの移動は一度だけ許可されている旨を示す。MVCNTIに示される移動許可回数は、このパッケージを受信したデジタルターミナルにより、”1”減じられた後、デジタルターミナルによりSDメモリカード１００に記録されることとなる。

【００４２】COCNTIの詳細設定を破線py2にて引き出して示す。001に設定された際、著作物のチェックアウトを一回だけ(1つの記録媒体に対してのみ)許可している旨を示す。002に設定された際、著作物のチェックアウトを2回だけ(2つの記録媒体について)許可し、003、004に設定された際、3つ、4つの記録媒体に対してチェックアウトを許可する旨を示す。

【００４３】PB_COUNTの詳細設定を破線py3にて引き出して示す。PB_COUNTは著作物を何秒再生すれば、著作物が1回再生されたとカウントするかを示すPlayback Time(Playback Time)と、著作物の再生を何回許可するかを示すPlayback Counter(Playback Counter)とからなる。続いて、著作物がSDメモリカード１００に記録される際、著作物を構成するデータセットがどのようなデータ構造に変換されるかについて説明する。SDメモリカード１００への記録時において、曲等、単体の著作物は、トラックという形態に変換されてSDメモリカード１００に記録される。トラックは、暗号化されたオーディオデータであるAudio Object（AOB）、暗号化された静止画データであるPicture Object（POB）、トラックについての再生制御情報であるTrack Informatin（TKI）を含み、著作物を構成する全てのデータは、種別を問わずトラックという単位で一律に管理されることとなる。

【００４４】また音楽アルバム等の著作物の集合体は、トラックシーケンスという形態に変換されて、SDメモリカード１００に記録される。トラックシーケンスは、複数のトラックと、それらトラックの再生順序を定義するプレイリストとからなる。SDメモリカード１００において、著作物をトラック、トラックシーケンスとして管理するためのデータ構造を図１２に示す。図１２は、著作物のデータセットを記録するために形成されるファイル、ディレクトリを示す図である。本図における矢印PF1,2,3,4,5,6,7は、パッケージに含まれる各データと、応用層の各ファイルとの対応関係を示す。

【００４５】本図においてユーザデータ領域には、Root、SD_Audio、SD_ADEXTディレクトリィといった3つのディレクトリが形成されている。このうち、SD_Audioディレクトリは SD-Audio Ver1.0規格に規定されたデータ、SD_ADEXTディレクトリィは、SD-Audio Ver1.1規格に固有

のデータを格納するディレクトリである。そのため、SD-Audio Ver1.0規格に対応する機器は、SD_Audioディレクトリに対してアクセスを行うが、SD_ADEXTディレクトリィに対してアクセスは行わない。一方、SD-Audio Ver1.1規格に対応する機器は、SD_Audioディレクトリ、SD_ADEXTディレクトリィの双方に対してアクセスを行う。尚、図中のxxxは、001から999までの整数値を示す。

【００４６】以降、SD_Audioディレクトリに配置されているファイルを順に説明してゆく。本図に示すように、SD_Audioディレクトリには、『AOBxxx.SA1』『POBxxx.SP1』『SD_AUDIO.TKM』『SD_AUDIO.PLM』『POBOOO.POM』といった5種類のファイルが配されている。『AOBxxx.SA1』は、パッケージに含まれる複数のCELのうち、AACストリームデータをAOBとして収録しているファイルである。『AOBxxx.SA1』における拡張子『SA』は、『Secure Audio』の略であり、これらの格納内容は、著作権保護の必要性があることを示す。

【００４７】続いてAOBファイルの内部構成について説明する。図１３は、AOBファイルのデータ構成を階層的に示す図である。本図の第１段目は、AOBファイルを示し、第２段目は、AOBを示す。第３段目は、AOB_BLOCKを示し、第４段目はAOB_ELEMENT、第５段目は、AOB_FRAMEを示す。図１３の第５段目における『AOB_FRAME』は、AOBを構成する最小単位であり、再生時間が約20ミリ秒となる可変符号長データである。

【００４８】第４段目に位置する『AOB_ELEMENT』は、再生時間が約2秒となる可変符号長データであり、そのデータ長がタイムサーチテーブルに示されている。第３段目に位置する『AOB_BLOCK』は、AOBの先頭部分、又は、終端部分に無効部分が存在する場合、それら無効部分を除いて有効部分のみを指示するデータであり、TKIの中のBITにて指定される。

【００４９】第２段目に位置するAOBは、8.4分の再生時間を上限としたデータである。各AOBを8.4分の再生時間に限定した理由は、AOBに含まれるAOB_ELEMENTの個数を制限することにより、タイムサーチテーブルのサイズを504バイト以下に抑制するためである。以下、再生時間の限定により、タイムサーチテーブルの抑制が可能となった理由を詳細に説明する。

【００５０】順方向サーチ再生、逆方向サーチ再生の再生を行う際、2秒分読み出しをスキップして240ミリ秒だけ再生するという『2秒スキップ240ミリ秒再生』が行われる。このように2秒という時間長をスキップする場合、その2秒間隔の読出先アドレスをタイムサーチテーブルに記述して、順方向サーチ再生及び逆方向サーチ再生が命じられた際、再生装置がこれを参照すればよい。2秒に相当するデータ長がどの程度になるかについて考察すると、オーディオデータの再生時のビットレートは、上述したように16Kbps～144Kbpsの範囲であるので、2秒当たりに再生されるデータ長は4Kbyte(=16Kbps×2／8)～36Kbyte(=144Kbps×2/8)となる。

【００５１】2秒当たりのデータ長が4Kbyte～36Kbyteであるなら、オーディオデータのデータ長が記述されるためのタイムサーチテーブル内のエントリーのデータ長は、2バイト(16ビット)必要となる。何故なら、エントリーに16ビット長を割り当てたならば、0～64KByteの数値が記述されることができるからである。一方、タイムサーチテーブルの総データサイズを例えば504バイト(これは後述するTKTMSRTのデータサイズである)内に制限する場合を考えると、このタイムサーチテーブル内に設けるべきエントリーは、252(=504/2)個に制限せねばならない。上述したように、エントリーは、2秒毎に設けられるものであるので252エントリーに対応する再生時間は、504秒(=2秒×252)となり、8分24秒(=8.4分)となる。このようにAOB_BLOCKにおける再生時間を8.4分以下に制限したことにより、タイムサーチテーブルのデータサイズを504バイト以下とすることができる。

【００５２】図１４は、AOBファイルに収録されている各AOB、AOB_BLOCKが連続して再生されることにより、どのような再生内容が再生されるかを示す。第１段目は、ユーザデータ領域における8つのAOBファイルを示し、第２段目は、各AOBファイルに収録されている8つのAOBを示す。第３段目は、それぞれのAOBに含まれる8つのAOB_BLOCKを示す。

【００５３】第５段目は、5つのパッケージからなるタイトルを示す。5つのパッケージは、SongA、SongB、SongC、SongD、SongEという5つの曲のそれぞれを示す。破線AS1,AS2,AS3　　AS7,AS8は、音楽アルバムの分割部分と、AOB_BLOCKとの対応関係を示し、第４段目は、第５段目の音楽アルバムがどのような単位で分割されるかを示す。

【００５４】AOB#4は、30.6分という時間にて再生される曲(SongD)の先頭部分であり、8.4分という再生時間にて再生される。AOB#5、AOB#6に含まれるAOB_BLOCKはSongDの中間部分であり、8.4分という再生時間、AOB#7に含まれるAOB_BLOCKは、SongDの終端部分であり、5.4分という再生時間にて再生される。このように30.6分という再生時間を有する曲は、(8.4分+8.4分+8.4分+5.4分)という単位で分割され、各AOBに含まれていることがわかる。この図からも理解できるように、AOBファイルに含まれる全てのAOBは、再生時間長が8.4分という時間長以内に収められていることがわかる。図１５は、図１４に示したタイトル（音楽アルバム）を格納した8つのAOBファイルを示す図である。

【００５５】『POBXXX.JPG/SP1』は、静止画データを収録したファイルであり、『POBXXX.JPG』『POBXXX.SP1』という2つのPOBXXX.JPGと、POBXXX.SP1の違いは、著作権の有無の相違である。前者は、単にJPEG方式の静止画データを収録したファイルであるのに対して、後者は、静止画の著作権を保護するため、暗号化されている点で

ある(その拡張子のSP1は"Secure Picture"の略であり、著作権保護の必要性があることはこれからも明らかである。)。

【００５６】『SD_Audio.TKM』は、パッケージのヘッダ、Navigation Structure、タイムサーチテーブルの内容を継承したデータであり、トラックマネージャ(Track Manager)を含む。図１６（ａ）は、Track Managerの構成を段階的に詳細化した図である。即ち、本図において右段に位置する論理フォーマットは、その左段に位置する論理フォーマットを詳細化したものであり、破線に示す引き出し線は、右段の論理フォーマットがその左段の論理フォーマット内のどの部分を詳細化したかを明確にしている。このような表記に従って図１６（ａ）におけるTrack Managerの構成を参照すると、Track Managerは、破線の引き出し線h1に示すように、n個のTrackInformation(TKIと略す)#1　　#nからなる。これらのTKIはAOBファイルに収録されているAOBを、トラックとして管理するための情報であり、各AOBファイルに対応している。

【００５７】図１６（ａ）を参照すると各TKIは、破線の引き出し線h2に示すように、Track_General_Information(TKGI)、アーティスト名、アルバム名、編曲者名、プロデューサ名等、TKIに固有なテキスト情報が記述されるTrack_Text_Infomation_Data_Area(TKTXTI_DA)、8.4秒という再生時間を上限としたタイムサーチテーブル(Track_Time_Serch_Table(TKTMSRT))からなる。

【００５８】図１７は、TKIと、図１４に示したAOBファイル及びAOBとの相互関係を示す図である。図１７の第１段目における四角枠はTrackA～Eとからなるトラック列（トラックシーケンス）、図１７の第２段目における四角枠はTrack Managerを示し、第３、第４段目は図１４に示した8つのAOBファイルを示す。第５段目における8つの枠は、8つのAOBを示す。この8つのAOBファイルは、図１４に示した8つのAOBを収録していたものであり、TrackA、TrackB、TrackC、TrackD、TrackEを含む音楽アルバムを形成している。第２段目は、8つのTKIを示す。これらTKIに付与された数値"1","2","3","4"は、各TKIを識別するためのシリアル番号であり、各TKIは、同じシリアル番号001,002,003,004,005　　が付与されたAOBファイルと対応づけられている。この点に注意して、図１７を参照すれば、TKI#1がAOB001.SA1に対応していて、TKI#2がAOB002.SA1、TKI#3がAOB003.SA1、TKI#4がAOB004.SA1に対応していることがわかる（本図における矢印TA1,TA2,TA3,TA4　　は、各TKIがどのAOBファイルと対応しているかを示す。）。このように各TKIは、各AOBファイルに収録されているAOBと、1対1の対応関係を有するので、各TKIには、AOBに固有な情報を詳細に記載しておくことができる。

【００５９】TKGIの詳細構成を図１６（ｂ）に示す。図１６（ｂ）に示すように、TKGIは、『TKI_ID』『TKIN』『TKI_BLK_ATR』『TKI_LNK_PTR』『TKI_SZ』『TKI_PB_TM』『TKI_AOB_ATR』『TKI_POB_ATR』『TKI_T11_ATR』『TKI_T12_ATR』『TKI_TMSRT_SA』『ISRC』『TKI_APP_ATR』『BIT』『TKI_POB_SRP』からなる。『TKI_ID』には、TKIを一意に識別できるID(本実施形態では2バイトの"A4"というコード)が記述される。

【００６０】『TKIN』には、1から999までの範囲のTKI番号が記述される。『TKI_BLK_ATR』には、TKIについての属性が記述される。図１７の一例では、それぞれのTKIについてのTKI_BLK_ATRがどのように設定されているかについて説明する。各TKIにおけるTKI_BLK_ATRを参照すれば、TKI#1（AOB001.SA1）、TKI#2（AOB002.SA1）、TKI#3（AOB003.SA1）、TKI#8（AOB008.SA1）という4つの組みは、それぞれが独立したトラックに対応しているので、TKI#1、TKI#2、TKI#3、TKI#8のTKI_BLK_ATRは、『Track』と設定されている。TKI#4におけるTKI_BLK_ATRは『Head_of_Track』と設定され、TKI#7におけるTKI_BLK_ATRは『End_of_Track』と、TKI#5、TKI#6は『Midpoint_of_Track』と設定されていることがわかる。このことは、TKI#4と対応関係を有するTKI#4（AOB004.SA1）はトラックの先頭部と、TKI#5、TKI#6と対応関係を有するTKI#5（AOB005.SA1）及びTKI#6（AOB006.SA1）はトラックの中間部と、TKI#7と対応関係を有するTKI#7（AOB007.SA1）はトラックの終端部であることを意味する。

【００６１】このTKI_BLK_ATRを設定することにより、複数のトラックのうち、任意の2つを1つのトラックに統合するという統合編集、1つのトラックを複数に分割するという分割編集が容易に行なえることとなる。トラックの統合を行う際の、TKIの更新について説明する。図１８（ａ）、（ｂ）は、2つのトラックを1つに統合する場合にTKIがどのように設定されるかを示す図である。図１８（ａ）において、TrackCとTrackEとを1つのトラックに統合するという編集操作を操作者が希望しているものとする。これらTrackC、TrackEに対応するAOBがAOB003.SA1、AOB008.SA1に収録されており、それらがTKI#3、TKI#8に対応づけられているので、これらTKI#3及びTKI#8のTKI_BLK_ATRの書き換えが行われる。図１８（ｂ）は、TKIのTKI_BLK_ATRの書き換え後を示す図である。図１８（ａ）においてTKI#3、TKI#8のTKI_BLK_ATRはTrackと記載されているが、図１８（ｂ）では、TKI#3のTKI_BLK_ATRは『Head_of_Track』に書き換えられ、TKI#8のTKI_BLK_ATRは『End_of_Track』に書き換えられている。このように、TKI_BLK_ATRが書き換えられることにより、TKI#3、TKI#8、これらに対応するAOB003.SA1、AOB008.SA1は、TrackCという1つのトラックとして扱われる。

【００６２】トラックの分割を行う際の、TKIの更新について説明する。図１９（ａ）、（ｂ）は、1つのトラックを2つのトラックに分割する場合を想定した図である。本図において、TrackCをTrackC－TrackFという2つ

のトラックに分割するという編集を操作者が希望しているものとする。TrackCをTrackC－TrackFに分割しようとすると、TrackFに対応するAOB002.SA1が生成される。図１９（ａ）では、TKI#2が『Unused』に設定されており、分割の結果、図１９（ｂ）に示すように『Unused』に設定されているTKI#2は、新たに生成されたAOB002.SA1に割り当てられる。

【００６３】『TKI_LNK_PTR』には、当該TKIのリンク先のTKIについてのTKINが記述される。図１７において矢印TL4,TL5,TL6に示すように、TrackDを構成する4つのAOBファイルに対応するTKI#4、TKI#5、TKI#6、TKI#7は、各TKI_LNK_PTRが次のTKI_LNK_PTRを指示するよう設定されている。『TKI_SZ』には、TKIのデータサイズがバイト数単位で記述される。

【００６４】『TKI_PB_TM』には、TKIに対応するAOBファイルに収録されているAOBにより構成されるトラック(曲)の再生時間が記述される。『TKI_AOB_ATR』には、TKIに対応するAOBファイルに収録されているAOBがどのようなサンプリング周波数でサンプリングされているか、どのようなビットレートで転送されるか、チャネル数がどれだけであるか等、AOBを生成する際のエンコード条件が記述される。

【００６５】『TKI_POB_ATR』は、POBをどのようなで態様で表示させるか（シーケンシャルモード、ランダムモード、シャッフルモードといった態様がある。）、POBの表示と、TKIに対応づけられているAOBファイルの再生とを同期させるか否か（スライドショー、ブラウザモードがある。）が設定されるフィールドである。『TKI_T11_ATR』,『TKI_T12_ATR』は、著作物と共に表示されるべきテキスト情報がどのような種類であるか（ISO646,JISX0201,ISO8859,Music Shift JIS漢字等がある。）を示す『TKI_TMSRT_SA』は、TMSRTの先頭アドレスが記述される。

【００６６】『ISRC』には、TKGIにおけるISRC（International Standard Recording Code）が記述される。『TKI_APP_ATR』は、本SDメモリカード１００に格納されるアプリケーションのジャンルが音楽ジャンルであるか、カラオケソフトであるか、プレゼンテーションデータであるかが記述される。

【００６７】『ブロック情報テーブル(BIT)』は、AOB_BLOCKを管理するテーブルである。図１６（ｂ）の右側に、BITの詳細構成を示す。図１６（ｂ）に示すように、BITは、DATA_OFFSETフィールドと、SZ_DATAフィールドと、FNs_1st_TMSRTEフィールドと、FNs_Last_TMSRTEフィールドと、FNs_Middle_TMSRTEフィールドと、TIME_LENGTHフィールドとからなる。以下、各構成要素の説明を行う。

【００６８】『DATA_OFFSET』には、クラスタ境界から各AOB_BLOCKの先頭までの相対アドレスがバイト単位で記述される。これにより、AOBからAOB_BLOCKまでの間に無効領域がどれだけ存在するかが表現される。AOBとしてSDメモリカード１００に格納されている音楽が、エアチェックして録音された音楽であり、その音楽のイントロの部分にディスクジョッキーの音声が混じっている場合、BITにおけるDATA_Offsetを設定することにより、この不要音声をAOB_BLOCKから除外して再生させないようにすることができる。

【００６９】『SZ_DATA』には、各AOB_BLOCKのデータ長がバイト単位で記述される。SZ_DATAとDATA_Offsetとを加算した値をAOBを収録しているファイルサイズ(クラスタサイズの整数倍)から差し引けば、AOB_BLOCKに後続する無効領域がどれだけのサイズであるかを求めることができる。つまり、AOBの後半に、再生不要な部分が存在する場合、このSZ_DATAを調整することにより、そのような後半部分の無効部分を再生させないようにすることができる。以上のDATA_OFFSET及びSZ_DATAを操作することにより、AOBの前後を部分削除することが可能となる。

【００７０】『FNs_1st_TMSRTE』には、当該AOB_BLOCK中の先頭に位置するAOB_ELEMENTに含まれるAOB_FRAME数が記述される。『FNs_Last_TMSRTE』には、AOB_BLOCKの最後尾のAOB_ELEMENTに含まれるAOB_FRAMEの個数が記述される。『FNs_Middle_TMSRTE』には、先頭と最後尾のAOB_ELEMENTを除くAOB_ELEMENT、即ち、AOB_BLOCKの中間部に位置するAOB_ELEMENTに含まれるAOB_FRAMEの個数が記述される。

【００７１】『TIME_LENGTH』は、AOB_ELEMENTの再生期間をミリ秒オーダーの時間精度で記述するフィールドである。TIME_LENGTHフィールドは、16ビット長であり、符号化方式がMPEG-AAC方式やMPEG-Layer3方式であれば、AOB_ELEMENTの再生期間は2秒となるので、TIME_LENGTHには、2000の値が記述される。図２０は、AOB_ELEMENT#1～#4からなるAOBが格納されているクラスタ007～クラスタ00Eを示す図である。AOBが図２０に示すように格納されている場合に、BITがどのように設定されるかについて説明する。本図におけるAOB_ELEMENT#1～#4は、クラスタ007の途中md0からクラスタ00Eの途中md4迄を占有している。BIT内のSZ_DATAは、矢印sd1に示すようにAOB_ELEMENT#1からAOB_ELEMENT#4の最後までを指示しており、BIT内のDATA_Offsetは、非占有部分ud0のデータ長、即ち、クラスタ007の先頭から、AOB_ELEMENT#1の先頭までの相対値を指示している。BITにより、クラスタ境界からAOB_ELEMENTまでのオフセットが管理されていることがわかる。

【００７２】『TKI_POB_SRP』は、Default_Playlist情報、PlayList情報により指定された再生順序により再生が行われている時間帯のうち、特定のAOBが再生される再生期間に表示すべきPOBを指定するフィールドである。言い換えれば、Track ManagerはTKI_POB_SRPを設定することにより、トラック毎に表示すべきPOBを指定す

ることができる。

【００７３】図２１は、Track Managerに含まれるTKI#2～TKI#4についてのTKI_POB_SRPの設定例を示す図である。第１段目は、Track Managerを示し、第２段目は、３つのPOBファイルを示す。第１段目におけるTrack Managerは、8つのTKIを含み、矢印は、それらTKI内のTKI_POB_SRPがどのPOBファイルを参照しているかを示す。矢印に示される参照関係によると、TKI#2,#3,#4のTKI_POB_SRPは、それぞれPOB001、POB002、POB003を指定している。POB001～POB003の内容は、TrackB,C,Dに関連するものであり、これらは何れも各トラックが再生されている期間に再生しないと意味がないので、TKIに含まれるTKI_POB_SRPにより、各トラックが再生されている期間において再生されるよう設定されている。

【００７４】以上でTKGIについて説明を終える。続いて、図１２の残りのファイルについての説明を引き続き行う。『SD_AUDIO.PLM』は、トラックの複数の再生順序を規定する情報であり、Default_Playlist_Track_Search_Pointer(DPL_TK_SRP)#1,#2,#3,#4　　#mを含む。図２２は、Default_Playlist情報、TKI、AOBファイルの相互関係を示す図である。本図のDefaultPlaylist内のDPL_TK_SRP#1,#2,#3,#4　　#8のDPL_TKINは、TKI#1,#2,#3,#4　　#8を示しているので、矢印(1)(2)(3)(4)(8)に示すように各AOBが再生されることになる。次に、Default_Playlist情報におけるDPL_TK_SRPの順序を入れ替えることにより、トラックの再生順序を変更するという編集操作がどう行われるかについて説明する。図２３（ａ）、（ｂ）は、トラックの順序を入れ替える場合を想定した図である。図２３（ａ）におけるDPL_TK_SRP、TKIの設定は、図２２と同じである。図２３（ａ）における再生順序は、TrackA、TrackB、TrackC、TrackD、TrackEであるが、図２３（ｂ）におけるDefault_Playlist情報では、DPL_TK_SRP#3、DPL_TK_SRP#8についてのDPL_TKINの順序が入れ替えられたので、TrackA、TrackB、TrackE、TrackD、TrackCの順序で再生されることになる。このように、Default_Playlist情報における、DPL_TK_SRPの順序を入れ替えることにより、簡易にトラックの再生順序を変更することができる。

【００７５】『POB000.POM』は、POBがTKGIにより指定されているか否か、指定されていればその指定回数等を、各POBの管理情報として示す情報である。以上でSD_Audioディレクトリに配置されたファイルについての説明を終え、続いてSD_ADEXTディレクトリィに配置されたファイルについて説明する。SD_ADEXTというディレクトリ名における"SD_AD"は、SD-Audio の略であり、EXTはExtensionの略である。すなわち、SD-Audio Ver1.1規格のために拡張されたディレクトリであることを表している。

【００７６】『STKIxxx.SDT』は、図２４の内部構成を有する"セキュアな"トラック情報(Secure Track Information)である。図２４を参照すると、STKIは、256バイトのSecure Track General Information（S_TKGI）と、256バイトのSecure Track TextInformation Data Area（S_TKTXTI_DA）とから構成されることがわかる。なお、STKIxxx.SDTファイルと、TKIとを比較すると、TKIに存在していたTKTMSRTがSTKIには、存在しないことがわかる。また互いのTKGIを比較すると、TKIのTKGIに存在していたTKI_TMSRT_SA、BITは、STKGIには存在せず、代わりにS_TKI_FR_ID1～4が存在することがわかる。データ構造の違いは以上の通りである。S_TKI_FR_ID1～4は、ID情報を記述するために設けられたフィールドであり、KIOSK端末ごとのIDや、配信方式のID、あるいはユーザごとのID等が記述される。

【００７７】以下、TKIとSTKIとの差違について説明する。STKIは、著作物の権利証がSDメモリカード１００からローカルストレージへと移動した際、AOBに付随してSDメモリカード１００からローカルストレージへと移動するという付随性を有している点が異なる。STKIの内部には、S_TKI_FR_ID1～4が存在しており、これにKIOSK端末毎のIDや、配信方式のID、あるいはユーザごとのID等が記述されているので、STKIは、配信されたコンテンツの購入証明のように用いられる。

【００７８】S_TKIファイルとAOBファイルは、ファイル名の3桁の数字部分を同一とすることによって１対１に対応する。図２５は、SD_Audioディレクトリに含まれる3つのAOB#1、AOB#2、AOB#3、2つのPOB001.SP1、POB002.SP1がSD_ADEXTディレクトリィに含まれる3つのSTKI001.SDT、STKI002.SDT、STKI003.SDTとどのように対応するかを示す図である。AOB、STKIは、矢印AS1,AS2,AS3に示すように同一のシリアル番号を有するもの同士が対応している。S_TKIファイル中のS_TKI_POB_SRPの設定に基づき、矢印PS1,PS2に示すようにPOBは、各STKIと対応づけられる。すなわち図２５の例であれば、STKI002.SDTファイル中のS_TKI_POB_SRPにて、POB001.SP1が指定され、STKI003.SDTファイル中のS_TKI_POB_SRPにて、POB002.SP1が指定される。

【００７９】以上でユーザデータ領域に配置されているファイルについての説明を終える。続いて、プロテクト領域に配置されているファイルについて説明する。図１２においてプロテクト領域には、『AOBSA1.KEY』、『POBSP1.KEY』が配置されたSD_Audioディレクトリ、『AOBSA1.URM』、『POBSP1.URM』が配されたSD_ADEXTディレクトリィが存在する。

【００８０】『AOBSA1.KEY』は、AOBを復号するための複数の暗号鍵(TitleKey)を収録している暗号鍵格納ファイルである。これらの暗号鍵は、パッケージのDefault Offerに含まれる複数のCEL Keyのそれぞれと対応している。『POBSP1.KEY』は、POBを復号するための複数の暗号鍵(TitleKey)を収録している暗号鍵格納ファイルである。これらの暗号鍵も、パッケージのDefault Offerに

含まれる複数のCEL Keyのそれぞれと対応している。

【００８１】『AOBSA1.URM』は、各AOBに対応づけられた権利証（Usage Rule）を収録した権利証格納ファイルである。図２６は、AOBSA1.URMの構成を示す図である。本図においてAOBSA1.URMファイルは、ID情報や、バージョン番号、ファイルサイズといった情報が記述されるヘッダ部である『Usage Rule Manager Information』と、Usage Rule Entry#1,#2,#3　　#n(図中では、n=8)から構成される。

【００８２】『POBSP1.URM』は、各POBに1対1に対応づけられた権利証(Usage Rule)を収録した権利証格納ファイルである。対応するデータがPOBである点は、AOBSA1.URMと異なっているが、そのデータ構造は、AOBSA1.URMと同一である。図２７は、SD_Audioディレクトリィの下にAOBファイルが8つ存在し、これらに対応する暗号鍵がAOBSA1.KEYに8つ収録され、これらに対応するUsage RuleがAOBSA1.URMに8つ収録されている場合、AOBSA1.KEYと、AOBSA1.URMと、AOBファイルとの対応を示す図である。

【００８３】暗号化されたAOBファイルは、暗号鍵格納ファイル及び権利証格納ファイルと、以下の一定の規則(1)(2)(3)に基づく対応関係を有する。

(1)暗号鍵格納ファイル及び権利証格納ファイルは、暗号化されたファイルが格納されているディレクトリと同じディレクトリ名に配置される。図２７のユーザデータ領域においてSD_Audioディレクトリに AOBファイルが配されており、暗号鍵格納ファイルもSD_Audioディレクトリに配されている。権利証格納ファイルは、SD_AudioディレクトリのサブディレクトリであるSD_ADEXTディレクトリィに配されていることからも、この規則に従った、ファイル配置が行われていることがわかる。

【００８４】(2)暗号鍵格納ファイル及び権利証格納ファイルには、データ領域におけるAOBファイルのファイル名の先頭3文字と、所定の拡張子「.KEY」「.URM」とを組み合わせたファイル名が付与される。図２８（ａ）、（ｂ）は、AOBSA1.KEY、AOBSA1.URMと、AOBファイルとの対応関係を示す図である。AOBファイルのファイル名が『AOB001.SA1』である場合、暗号鍵格納ファイルには、矢印nk1,nk2に示すように、この先頭３文字『AOB』と、『SA1』と、拡張子『.KEY』とからなる『AOBSA1.KEY』というファイル名が付与されることがわかる。権利証格納ファイルには、矢印nk3,nk4に示すように、この先頭３文字『AOB』と、『SA1』と、拡張子『.URM』とからなる『AOBSA1.URM』というファイル名が付与されることがわかる。

【００８５】(3) AOBファイルのファイル名には、暗号鍵格納ファイル及び権利証格納ファイル内において、そのオーディオオブジェクトに対応するTitle key及びUsage Ruleが何番目に位置するか、即ち、対応するTitleKey及びUsage Ruleの順位を示すシリアル番号が付与される。AOBファイルのファイル名には、"001","002","003","004"といったシリアル番号が付与されている。これらのAOBファイル内のシリアル番号は、対応するTitle Key及びUsage Ruleがファイルにおいて何番目に位置するかを意味するので、各AOBファイルを暗号化する際に用いたTitle Key及びUsage Ruleは、同一のシリアル番号を有する『Title Key Entry』『Usage Rule Entry』に存在することとなる。図２７における矢印AK1,AK2,AK3,AK4は、AOBファイルとTitleKey、Usage Ruleとの対応関係を示す。

【００８６】続いてTitle Key Entryの内部構成について説明する。図２９はTitle Key Entryの内部構成を示す図である。図２９に示すように、Title Key Entryは、7バイトの暗号鍵『EKEY』、『Availability Flag』、『Content ID』とからなる。『Availability Flag』は、SDメモリカード１００において著作物が存在し、かつ当該エントリに有効な暗号鍵を記述する際、"1"に設定され、著作物がSDメモリカード１００からローカルストレージと移動した際、"0"に設定されるフラグである。

【００８７】『Content ID』は、コンテンツごとにユニークに割り振られる情報である。またAvailability Flagは、Content_IDと共に以下のように併用される。空きのTitle Key EntryにおけるContent_IDは"0"、空きでないTitle Key EntryにおけるContent_IDは（空きでないTitle Key Entryとは、Title Key Entryに対応するAOBファイルが存在することをいう。）、1～999と設定される。更にトラックとTKI(AOB)が1対多で対応する場合、AOBに対応するTitle Key EntryにおけるContent_IDが、全て同一の値となる。一方Availability Flagは、トラックとTKI(AOB)が1対1で対応する場合"1"に設定される。トラックとTKI(AOB)が1対多で対応する場合、多のTitle Key Entryのうち、唯一のものAvailability Flagが"1"に設定される。残りのTitle Key EntryのAvailability Flagは"0"に設定される。Content_IDが"0"ではなく、Availability Flagが"0"に設定されていれば、同一のContent_IDを有するTKI（AOB）が複数存在し得るから、これをきっかけに同一のContent_IDを有するTitle Key Entryを検出する。そうして1つのContent_IDに対応する複数のTKI（AOB）を特定するというサーチ処理が可能となる。

【００８８】続いてUsage Ruleについて説明する。図２６の右半分にUsage Ruleの構成を示す。各AOBに対応するUsage Ruleのフォーマットは図２６の右半分に表され、『C_HASHフィールド』、『Check-Out Control Information(制御情報)』、『Move Control Information(制御情報)』、『Trigger Bit』、『Content_IDフィールド』、『Availability Flag』、『STI_KEY』からなる。図中の"｛"記号にも示されているように、Content ID、Availability Flag、STI_KEYは、図２９に示したTitle

Key Entryの構成と同様である。

【００８９】『C_HASHフィールド』は、Enc-STKI、Enc-STI_KEY、Enc_AOBを連結して、SHA-１（Secure Hash Algorithm）に適用することにより得られる演算結果のうち、下位64ビットが書き込まれる（"Enc_"というのは、暗号化がなされているという意味である。）。ハッシュ関数とは一方向性関数であり、入力値の一部でも変化すると、出力値は大きく異なるという特徴を有する。さらに、入力値から出力値（ハッシュ値）を類推するのは非常に困難という特徴も有する。このC_HASHフィールドに書き込まれた値は、カスタマーズデバイスがSDメモリカード１００をアクセスする際、Enc-STKI、Enc-STI_KEY、Enc_AOBが「他のデータ」にすり変えられたか否かの検証に用いられる。

【００９０】即ち、SDメモリカード１００がカスタマーズデバイスに接続されると、カスタマーズデバイスはEnc-STKI、Enc-STI_KEY、Enc_AOBを連結して、これを下記のようにSHA-1アルゴリズムに適用し、64ビットのC_HASH-Ref値を得る。このようにして得たC_HASH-Ref値と、Usage RuleのC_HASHフィールドに書き込まれたC_HASHとの照合を行う。Enc-STKI、Enc-STI_KEY、Enc-AOBがデジタルターミナルによ りSDメモリカード１００に記録された時点と同じものなら、C_HASH-Ref値はUsageRuleに書き込まれているものと同じ値となるが、Enc-STKI、Enc-STI_KEY、Enc_AOBが改竄されたり、他のものにすり返られているなら、算出されるべきC_HASH-Ref値は、Usage Rule ManagerのC_HASHに記載されているものと大きく異なることとなる。このような照合をカスタマーズデバイスに行わせる目的で、C_HASHフィールドはUsage Rule Managerに設けられている。

【００９１】『Check-Out制御情報』は、SDメモリカード１００がカスタマーズデバイスに接続され、Usage RuleがSDメモリカード１００からローカルストレージに移動した際、幾つの記録媒体に、このUsage Ruleに対応するAOB、Title Keyの組みを記録させるかを示す。『Move制御情報』は、SDメモリカード１００からローカルストレージへの権利移動（記録を管理する権利の移動）が許可されているか否かを示す情報である。"1"に設定された場合、当該権利移動が1回だけ許可されている旨を示し、"0"に設定された場合、許可回数は0回であり、当該権利移動が禁止されている旨を示す。Move制御情報に示される移動許可回数は、このUsage Ruleを有するSDメモリカード１００と接続したカスタマーズデバイスにより、"1"減じられた後、カスタマーズデバイスによりローカルストレージに記録されることとなる。

【００９２】『Trigger Bit』は、"0"に設定されれば、権利移動を、Move制御情報のみで判断してよいかを示し、"1"に設定されれば、権利移動の可否は、Move制御情報だけでなく、他の情報を参照して総合的に行うべき旨を示す。Trigger Bitが設けられているのは、将来のUsage Ruleの機能拡張に備えるためである。即ち、著作物の移動の可否を判断するにあたって、Move制御情報だけでなく、他の要件の組み合わせで、判断を行いたいという要望が将来生じるかもしれない。そうした要望が生じた際には、Trigger Bitを"1"に設定しておき、その要件の成立と、Move制御情報の1の設定とが同時に満たされた場合に、著作物の移動を行わせる。

【００９３】以上で応用層のデータについての説明を終える。続いて、SDメモリカード１００からローカルストレージへと著作物の移動が行われる際、これまでに説明したファイルがどのように移動するかについて説明する。図３０（ａ）、（ｂ）は、著作物を構成するデータセットがSDメモリカード１００からローカルストレージにどのように移動するかを示す図である。ユーザデータ領域に配置されたファイルのうち、AOBファイル、POBファイル、STKIファイルは矢印MY1,MY2,MY3に示すように、SDメモリカード１００のユーザデータ領域から、ローカルストレージのユーザデータ領域へと読み出されることとなる。その後、SDメモリカード１００におけるAOBファイル、POBファイル、STKIファイルは、削除されることとなる。一方、SDメモリカード１００におけるプロテクト領域では、AOBSA1.KEY、POBSP1.KEY、AOBSA1.URM、POBSP1.URMは矢印MY4,MY5,MY6,MY7に示すように、ローカルストレージにおけるプロテクト領域に読み出されることとなる。

【００９４】図３０（ａ）、（ｂ）は、SDメモリカード１００におけるユーザデータ領域のオーディオオブジェクトを全てローカルストレージに移動させるケースを想定していたが、ユーザデータ領域における8つのAOBのうち、3つのみを移動させようとする場合、SDメモリカード１００のユーザデータ領域にどのようなファイルが配置されるかを図３１（ａ）、（ｂ）に示す。図３１（ａ）において、SDメモリカード１００のユーザデータ領域と、プロテクト領域からAOB#1～#3、Title KeyEntry#1～#3、Usage Rule Entry#1～#3がユーザデータ領域と、プロテクト領域から削除され、かわって図３１（ｂ）に示すように、ローカルストレージのユーザデータ領域と、プロテクト領域には、AOB#1、AOB#2、AOB#3、Title Key Entry#1～#3、Usage Rule Entry#1～#3が配置されることとなる。

【００９５】図３２は、図２５に示したAOBファイル、POBファイル、STKIファイルがSDメモリカード１００からローカルストレージへとどのように移動するかを示す図である。本図に示すように、SDメモリカード１００におけるAOB001.SA1、AOB002.SA1、AOB003.SA1、POB001.SP1、POB002.SP1、STKI001.SDT、STKI002.SDT、STKI003.SDTはSDメモリカード１００から削除され、かわって、ローカルストレージにこれらのファイルが配置されていることがわかる。以上で、応用層におけるディレクトリ構成、ファイル構成についての説明を終える。ローカルス

トレージにおいて、SDメモリカード１００と同様のディレクトリ構造を有しているが、流通時のフォーマットに示したフォーマット、即ち、図１０に示したタイトル及びパッケージらなるフォーマットに変換して記憶しておいても良い。続いて、デジタルターミナルの構成について説明する。

【００９６】図３３は、KIOSK端末型デジタルターミナルの構成を示す図である。本図に示すようにKIOSK端末型デジタルターミナルは、音楽会社からリリースされている著作物からなるホームライブラリィを閲覧するためのリリースコンテンツブラウザ部２１と、著作物に対する検索操作や著作物についての購入操作を操作者から受け付けるタッチパネル２２と、光ファイバー等の専用回線との接続を行い、専用回線を介した著作物の送受信を行う通信部２３と、PCMCIAのカードアダプタで構成され、SDメモリカード１００との間の入出力を行うカードコネクタ２４と、コインベンダを用いた現金受け取りや、キャッシュカード、ICカードを用いたオンライン決済を行うことにより、ユーザに対する課金を行う課金部２５と、SDメモリカード１００のプロテクト領域をアクセスするにあたって、必要な暗号化処理、復号化処理を実行するセキュア処理部２６と、KIOSK端末における販売サービスの統合制御を行う販売サービス制御部２７とからなる。

【００９７】図３４（ａ）は、パソコン型カスタマーズデバイスの構成を示す図である。デジタルターミナルは、ユーザがKIOSK端末から購入した著作物、ネットワークルートで購入した著作物からなるホームミュージックライブラリィを記録するローカルストレージ３２と、公衆回線との接続を行い、公衆回線を介して著作物の送受信を行う通信部３３と、PCMCIAのカードアダプタで構成され、SDメモリカード１００との間のデータ入出力を行うカードコネクタ３４と、ホームライブラリィに対するブラウザ機能を有するホームライブラリィブラウザ部３５と、操作者から操作を受け付ける入力受付部３６と、ローカルストレージ３２に構築されているホームライブラリィに新たな著作物を加える処理や、ローカルストレージに含まれる著作物を他の記録媒体にチェックアウトする処理を操作者からの操作に従ってを行うライブラリィ管理部３７と、SDメモリカード１００のプロテクト領域をアクセスするにあたって、必要な暗号化処理、復号化処理を実行するセキュア処理部３８とからなる。

【００９８】続いてSD-AUDIOプレーヤ１２２～１２４の内部構成を、図３４（ｂ）を参照しながら説明する。図３４（ｂ）に示すように、SD-AUDIOプレーヤ１２２～１２４は、PCMCIAのカードアダプタで構成され、SDメモリカード１００との間のデータ入出力を行うカードコネクタ６０、TitleKeyを用いてAOBファイルの暗号化を解除するデ スクランブラ６１、AOBファイルを復号することにより、PCMデータを得るAACデコーダ６２、AACデコーダ６２の復号により得られたPCMデータをD/A変換して、ヘッドホン端子を介してスピーカーに出力するD/Aコンバータ６３、SD-AUDIOプレーヤ１２２～１２４の処理を統合する制御部６４からなり、カスタマーズデバイスのチェックアウトによってSDメモリカードに記録されたトラック、又は、移動不可と設定されたUsage Ruleと共に、SDメモリカード１００に記録されたトラック、移動可能と設定されたUsage Ruleと共に、SDメモリカード１００に記録されたトラックを再生する。著作物の再生は、SD-AUDIOプレーヤ１２２～SD-AUDIOプレーヤ１２４によりなされるものとして説明したが、カスタマーズデバイス自身に図３４（ｂ）の内部構成を具備させて、著作物の再生を行わせてもよい。

【００９９】また、デジタルターミナルやカスタマーズデバイスにおける操作者の操作の受け付けは、タッチパネル以外にも、キーボードやマウス、トラックボール、スライドパッド、又はこれらの組み合わせで行ってもよい。更にリリースコンテンツブラウザ部２１、ホームライブラリィブラウザ部３５は、CRTやプラズマディスプレィ、液晶ディスプレィ等で、上述したコンテンツの閲覧を行わせてもよい。

【０１００】続いてデジタルターミナルに内蔵されているセキュア処理部２６の構成について説明する。図３５に示す通りセキュア処理部２６は、MKB処理部４１、ID処理部４２、AKE処理部４３、Kmu暗号化部４４、STI暗号化部４５、Ks暗号化部４６からなる。MKB処理部４１は、SDメモリカード１００のシステム領域に格納されているMKBと、デジタルターミナルの製造メーカーにより付与されたデバイス鍵Kdとを読み出し、これらを用いて所定の演算を行うことにより、56ビットの暗号鍵KmをID処理部４２に出力する。

【０１０１】ID処理部４２は、MKB処理部４１から56ビットの暗号鍵Kmが出力されれば、SDメモリカード１００のシステム領域からMedia-IDを読み出して、所定の演算を行うことにより、64ビットの演算結果を算出し、そのうち下位56ビットを暗号鍵Kmuとして、AKE処理部４３及びKmu暗号化部４４に出力する。AKE処理部４３は、ID処理部４２により算出された暗号鍵Kmuと、SDメモリカード１００側の暗号鍵Kmuとを用いたAKEプロセスを行う。その結果として得られた56ビットのセッション鍵KsをKs暗号化部４６に出力する。

【０１０２】Kmu暗号化部４４は、STI_KEY(図中では、KSTIと表記している)をランダムに選び、そのSTI_KEYを、ID処理部４２が出力した暗号鍵Kmuを用いて暗号化してKs暗号化部４６に出力する。また、Enc-STKI、Enc-STI_KEY、Enc_AOBを集めて、アルゴリズムSHA-1に適用することにより、C_HASH値を算出する。暗号化されたSTI_KEYと、C_HASH値とが得られると、C_HASH値をUsage Ruleに書き込んで、そのUsage Ruleを暗号鍵Kmuを用いて暗号化してKs暗号化部４６に出力する。

【０１０３】STI暗号化部４５は、STI_KEYを用いてSTKIを暗号化し、SDメモリカード１００に出力し、ユーザデータ領域に書き込ませる。Ks暗号化部４６は、AKE処理部４３から出力された56ビットのセッション鍵Ksを用いて、STKIとUsage Ruleとの組みを暗号化して、SDメモリカード１００に出力し、プロテクト領域３に書き込ませる。

【０１０４】以上で、デジタルターミナルにおけるセキュア処理部２６の構成についての説明を終える。続いて、カスタマーズデバイスにおけるセキュア処理部３８の構成について説明する。セキュア処理部３８の内部構成は、図３６に示す通りであり、MKB処理部５１、ID処理部５２、AKE処理部５３、Ks復号化部５４、Kmu復号化部５５、STI復号化部５６からなる。

【０１０５】MKB処理部５１は、SDメモリカード１００がカスタマーズデバイスに接続されると、システム領域１からMKBを読み出し、デバイス鍵Kdを用いて読み出されたMKBに対して所定の演算を行うことにより、56ビットの暗号鍵Kmを得る。ID処理部５２は、接続されたSDメモリカード１００のシステム領域１からMedia-IDを読み出し、MKB処理部５１により算出された暗号鍵Kmと、読み出されたMedia-IDとを用いて所定の演算を行い、64ビットの演算結果を得て、そのうち下位56ビットを暗号鍵Kmuとして、AKE処理部５３とKmu復号化部５５とに出力する。

【０１０６】AKE処理部５３は、Ks復号化部５４により出力された暗号鍵Kmuを用いて、SDメモリカード１００におけるAKE処理部５とAKEプロセスを行い、その結果である56ビットのセッション鍵KsをKs復号化部５４に出力する。Ks復号化部５４は、プロテクト領域に格納されているEnc-STKIとEnc-Usage Ruleとの組みであって、暗号化されたものをSDメモリカード１００から読み出し、AKE処理部５３が出力した56ビットのセッション鍵Ksを用いて復号する。そしてその結果をKmu復号化部５５に出力する。

【０１０７】Kmu復号化部５５は、ID処理部５２により算出された56ビットの暗号鍵Kmuを用いて、復号化を行い、STKIとUsage Ruleとの組みを得る。STI復号化部５６は、ユーザデータ領域からEnc-STI_KEYを読み出し、AKE処理部５３から出力されたSTI_KEYを用いて、読み出されたEnc-STKIの復号化を行って、STKIを得る。

【０１０８】以上説明したセキュア処理部２６、セキュア処理部３８による復号化、暗号化はC_CBC(Converted Cipher Block Chaining)モードで行われる。暗号化されたデータが512Byteであるとすると、C_CBCモードでは、このデータの8バイト部分を1つのブロックとして扱い、先頭の8バイトのブロックを7バイトの暗号鍵Mkを用いて復号する。その結果得られた8バイトの演算結果を、部分鍵として保持しておき、次の8バイトブロックの復号化に用いる。こうして512Byteのデータは8バイト単位に、復号化されてゆく。

【０１０９】また、AKEプロセスによるセッション鍵Ksの共有、SDメモリカード１００からの暗号化データの読み出し、セッション鍵Ksを用いた暗号化データの復号化、暗号鍵Kmuを用いた暗号化データの復号化といった一連の処理をセキュアリードといい、機器がSDメモリカード１００に対して所定のリードコマンド（セキュアリードコマンド）を発行した際、これらの処理は順次実行される。

【０１１０】更に、暗号鍵Kmuを用いた暗号化データの暗号化、AKEプロセスにより得られたセッション鍵Ksを用いた暗号化データの暗号化、暗号化後のデータ送信といった一連の処理をセキュアライトといい、機器がSDメモリカード１００に対して所定のライトコマンド（セキュアライトコマンド）を発行した際、これらの処理は順次実行される。以上でセキュア処理部２６、セキュア処理部３８の内部構成についての説明を終える。

【０１１１】続いて、デジタルターミナル、カスタマーズデバイスの処理を統合する制御部である販売サービス制御部２７、ライブラリィ管理部３７について説明する。販売サービス制御部２７は、デジタルターミナルの統合制御を行うよう記述された実行形式プログラムを記憶したROMと、RAMと、CPUとからなる。この実行形式プログラムの処理手順を記載したのが、図３７、図３８のフローチャートである。以降、これらのフローチャートを参照しながら、販売サービス制御部２７の制御内容について説明する。図３７のフローチャートの処理が開始されれば、ステップＳ１において、販売サービス制御部２７は音楽会社からリリースされている著作物を紹介する一覧画面をリリースコンテンツブラウザ部２１に表示させた後、ステップＳ２～ステップＳ３を繰り返し行うループ処理に移行する。ステップＳ２では、著作物の購入を求める旨の操作が操作者から行われたかを判定し、ステップＳ３では、著作物の検索を求める旨の操作が操作者から行われたかを判定する。検索が要求されたなら、ステップＳ３においてYesとなり、ステップＳ４に移行する。ステップＳ４において、アーティスト名、曲名等のキーワード入力をタッチパネル２２を介して操作者から受け付け、ステップＳ５において通信部２３を介して、配信サーバー１０３をアクセスすることにより、キーワードに該当する著作物についての情報を配信サーバー１０３から検索する。そして、ステップＳ６において検索された著作物を示す一覧画面をリリースコンテンツブラウザ部２１に表示させた後、ステップＳ２～ステップＳ３からなるループ処理に戻る。

【０１１２】操作者により購入が要求されたなら、ステップＳ２がYesになってステップＳ７に移行し、課金部２５に対する現金支払が行われるのを待つ。硬貨がコインベンダーに投入されたなら、販売サービス制御部２７はステップＳ８において選択された著作物についてのパ

ッケージの送信要求を通信部２３に送信させる。その後、ステップＳ９においてパッケージの受信待ちを行い、ステップＳ１０では、パッケージを正常に受信したかを判定する。正常でなければ、ステップＳ８に移行し、送信要求を通信部２３に再度出力させる。通信部２３がパッケージを正常に受信したなら、ステップＳ１１においてパッケージをSD-AudioVer1.1形式に変換しつつSDメモリカード１００に記録する。ステップＳ１２では、SDメモリカード１００へのデータ記録が正常に行われたか否かを判定し、否ならば、ステップＳ１４において現金払い戻しを行う。正常に行われたならばステップＳ１３において、課金部２５に決済処理を行わせる。その後、ステップＳ１に移行し、初期画面表示をリリースコンテンツブラウザ部２１に行わせて、ステップＳ２～ステップＳ３からなるループ処理に移行する。

【０１１３】ステップＳ１１において、SD-Audio Ver1.1形式への変換がどのように行われたかを図３８のフローチャートを参照しながら詳細に説明する。SDメモリカード１００に著作物を記録しようとする場合、SDメモリカード１００中のユーザ領域のSD_AUIDOディレクトリをアクセスし、AOBxxx.SA1ファイルを読み出し、サーチし、空き番号があるかどうか判定する。もしも、AOBxxx.SA1ファイルがすでに999個存在する場合は、コンテンツをこれ以上記録できない旨を表示し、終了する。999個未満なら、ステップＳ２１において、販売サービス制御部２７はパッケージのCELに含まれるAACストリームデータを複数のAOBファイルに分割して、SD-AUDIOディレクトリに記録する。その後、ステップＳ２２において、販売サービス制御部２７は、SDメモリカード１００のユーザデータ領域に格納されているTrack Managerをオープンし、各AOBファイルに対応するTKIをTrack Manager内に生成する。ステップＳ２３では、パッケージに含まれるヘッダ、Navigation Structureに基づいた内容をTrack Manager内の複数TKIに設定する。続いてステップＳ２４において販売サービス制御部２７は、静止画データを複数のPOBファイルと、POMとに変換し、SDメモリカード１００に記録する。ステップＳ２５では、タイムサーチテーブルを分割して、対応するTKI内のTKTMSRTとして設定し、ステップＳ２６において販売サービス制御部２７は、Navigation Structureに基づいて、Playlist上におけるDPL_TK_SRPを設定する。以上で、SDメモリカード１００のユーザデータ領域のSD_Audioディレクトリに配置されるべきデータセットが設定されたこととなる。

【０１１４】以降、ステップＳ９０に移行して、DRMのMove制御情報に示されるMove許可回数は0であるかを否かを判定する。"0"であれば、ステップＳ２７～ステップＳ３３、ステップＳ９１の処理をスキップしてステップＳ３５に移行し、1つ以上ならステップＳ２７に移行する。次にステップＳ２７において販売サービス制御部２７は、Title Key Managerに生成された複数TKIに基づいて、複数のSTKIを生成する。ステップＳ２８では、複数のSTI_KEYを生成し、これらを用いて各STKIを暗号化した後、SD_ADEXTディレクトリィに記録する。ステップＳ２９において販売サービス制御部２７は、SDメモリカード１００からUsage Rule Managerをセキュアリードし、ステップＳ３０において各販売サービス制御部２７は、AOBに対応するUsage RuleをUsage Rule Managerに生成する。ステップＳ９１においてMove許可回数のデクリメントを行い、ステップＳ３１において。デクリメントされたMove許可回数と、CheckOut制御情報とを各Usage Ruleに設定する。ステップＳ３２においてSTKIの暗号化に用いたSTI_KEYをUsage RuleのSTI_KEYフィールドに設定する。ステップＳ３３では、SDメモリカード１００にUsage Rule Managerをセキュアライトする。以上の処理にて、STKI、Usage Rule Managerが記録されたので、SD-Audio Ver1.1規格対応のデータがSDメモリカード１００に設定されたこととなる。

【０１１５】続いて、ステップＳ３５では、SDメモリカード１００からTitle Key Managerをセキュアリードし、ステップＳ３６において販売サービス制御部２７は、Default Offer内のCEL Key Chainに含まれるCEL KeyをAOBSA1.KEYの各AOBに対応するTitle Key Entryに書き込む ステップＳ３７において販売サービス制御部２７は、CEL Keyが書き込まれたTitle Key ManagerをSDメモリカード１００にセキュアライトする。

【０１１６】以上でデジタルターミナルにおける販売サービス制御部２７についての説明を終える。続いてカスタマーズデバイスについてのライブラリィ管理部３７について詳細な説明を行う。ライブラリィ管理部３７は、カスタマーズデバイスの統合制御を行うよう記述された実行形式プログラムを記憶したROMと、RAMと、CPUとからなる。この実行形式プログラムの処理手順を記載したのが、図３９～図４１のフローチャートである。以降、これらのフローチャートを参照しながら、ライブラリィ管理部３７の制御内容について説明する。図３９のフローチャートの処理が開始されれば、ライブラリィ管理部３７はステップＳ４１においてローカルストレージ３２に格納されているトラックの一覧表示を行い、ステップＳ４２～ステップＳ４５を繰り返し行うループ処理に移行する。ステップＳ４２においてライブラリィ管理部３７は、SDメモリカード１００からローカルストレージ３２へのトラック移動が要求されたかの判定を行い、ステップＳ４３では、トラックのチェックアウトが要求されたかの判定、ステップＳ４４では、トラックのチェックインが要求されたかの判定、ステップＳ４５では、サーバコンピュータからの著作物購入が要求されたかの判定を行う。

【０１１７】サーバコンピュータからの著作物購入が要求された場合、ステップＳ４５がYesとなってステップＳ４６に移行する。ステップＳ４６においてライブラリ

ィ管理部３７は通信部３３にダウンロード要求を送信させ、ステップＳ４７においてパッケージの受信待ちを行う。パッケージの受信を行えば、図３７のフローチャートに示したデジタルターミナルの処理と同様の処理を行って、ステップＳ４８において受信したパッケージをローカルストレージ３２に格納し、その後、ステップＳ４２～ステップＳ４５に移行する。

【０１１８】SDメモリカード１００からローカルストレージ３２へとトラックを移動する処理が要求されたなら、ステップＳ４２がYesとなり、図４１のステップＳ７１に移行して、ライブラリィ管理部３７は、SDメモリカード１００からUsage Rule Managerをセキュアリードする。以降、このSDメモリカード１００において格納されている複数のトラックのそれぞれを変数#xにて指示するものとする。以降、ステップＳ７２において#xに初期値を代入し、ステップＳ７３においてライブラリィ管理部３７は、Usage Rule#xのTrigger Bitをチェックする。Trigger Bitが"1"なら、次のトラックに処理を移すよう、ステップＳ７９に移行して変数#xをインクリメントした後、ステップＳ７３に移行する。Trigger Bitが"0"なら、ステップＳ７４においてライブラリィ管理部３７は、Usage Rule#xのMove制御情報をチェックする。Move制御情報に示される移動許可回数が"0"ならそのトラックをローカルストレージ３２に移動することは禁じられているので、次のトラックに処理を移すよう、ステップＳ７９に移行して変数#xをインクリメントした後、ステップＳ７３に移行する。Move制御情報が"1"であれば、ステップＳ７５に移行する。

【０１１９】ステップＳ７５では、Enc-STKI#x、Enc-STI_KEY#x、Enc_AOB#xを連結して、C_HASH-Ref値#xを得る そして、ステップＳ７６においてライブラリィ管理部３７は、C_HASH-Ref値#xと、Usage Rule#xにおけるC_HASH#xとが一致か否かを判定する。一致しなければ、ステップＳ７９に移行するが、一致するのであれば、ステップＳ８０において、Usage Rule#xにおいてMove制御情報に示されるMove許可回数をデクリメントし、ステップＳ８１において、デクリメントされたMove許可回数と、CheckOut制御情報とを含むUsage Rule#xをローカルストレージにセキュアライトする。続いてステップＳ７７では、SDメモリカード１００におけるUsageRule#xのAvailability Flagに"0"を、Content IDに"0"をセキュアライトし それ以外のUsage Rule#xのフィールド（STI_KEYを含む）に乱数をセキュアライトすることにより、Usage Rule#xをSDメモリカードから削除する。加えて、SDメモリカード１００においては、SD_AUDIO.TKMファイル中のTKI#xを無効にし、さらには、SD_AUDIO.PLMファイル中のデフォルトプレイリストから、TKI#xに関連する情報を削除する。また、POB000.POMファイルに対しては、TKI#xにて参照されているPOBファイルの参照カウンタを１減算する。Move時にこのカウンタが０となった場合は、当該POBファイルを削除する。

【０１２０】その後、ステップＳ８２において、トラック#xを構成するAOB#x,STKI#xをSDメモリカード１００におけるユーザデータ領域から読み出して、ローカルストレージ３２におけるユーザデータ領域に記録する。ステップＳ８３においてAOB#xについてのTitle_Key_EntryをSDメモリカード１００におけるプロテクト領域からセキュアリードして、ローカルストレージ３２におけるプロテクト領域にセキュアライトする。以上で、トラック#xを構成するデータセットは、ローカルストレージ３２に格納されたことなる。

【０１２１】その後、ステップＳ７８においてライブラリィ管理部３７は、変数#xがUsageRule Managerにおけるラストナンバーか否かを判定し、そうでないならステップＳ７９において#xをインクリメントした後、ステップＳ７３に移行する。これらの処理をAOBSA1.URMに含まれる全てのUsage Ruleについて繰り返せば、SDメモリカード１００において移動が可能なように設定されている全てのトラックは、SDメモリカード１００からローカルストレージ３２へと移動することとなる。配信サーバー１０３からの著作物購入、又は、SDメモリカード１００からの著作物の移動により、カスタマーズデバイスにおけるローカルストレージ３２には、多くの著作物が蓄積され、ホームライブラリィが構築されることとなる。

【０１２２】トラックのチェックアウトが要求された場合、図３９のステップＳ４３がYesとなり、図４０のステップＳ６６に移行する。ステップＳ６６では、SDメモリカード１００以外の他の記録媒体に記録すべきトラックの選択待ちを行い、選択されれば（選択されたトラックをトラック#xと呼ぶ。）、ステップＳ１００においてライブラリィ管理部３７は、カスタマーズデバイスに接続されたSDメモリカード１００に固有なMedia-IDを読み出す。一方、このSDメモリカード１００における空きのContent_IDを探し出して、選択されたトラックにこの空きのContent_IDを割り当てて、Media-IDと、Content_IDとの組みをチェックアウト履歴情報として記憶する。その後、ステップＳ４９においてトラック#xに対応するUsage Rule#xのセキュアリードを行う。ステップＳ５０では、Usage Rule#xにおいてCheck-Out制御情報に示されている回数(Check Out回数という)が"0"であるか否かを判定する。Check Out回数が"0"であれば、ステップＳ５１～ステップＳ５７の処理をスキップしてステップＳ４２～ステップＳ４５の処理に移行するが、"0"でなければ、ライブラリィ管理部３７はステップＳ５１においてトラック#xを構成するデータセット（Usage Ruleを除く）を他の記録媒体に記録する。チェックアウト時において、可搬型記録媒体には、図１２に示したようなディレクトリ構成、ファイル構造のうち、SD-Audio Ver1.0規格に規定されたもの、即ち、『AOBxxx.SA1』『POBxxx.SP1』『SD_AUDIO.TKM』『SD_AUDIO.PLM』『POB000.PO

M』、『AOBSA1.KEY』、『POBSP1.KEY』が記録される。これにより、トラックが記録されることとなる。そのためトラック統合、トラック分割といったトラック編集や、順方向、逆方向サーチ再生が可能となる。

【０１２３】続いてステップＳ５２においてCheck Out回数をデクリメントし、ステップＳ５３では、Check Out回数が"0"であるか、1以上であるか否かを判定する。CheckOut回数が"0"であれば、ステップＳ５４において、トラックを"チェックアウト不可能"に設定した後、ステップＳ５５に移行する。Check Out回数が"1"以上であれば、ライブラリィ管理部３７は、ステップＳ５５において、デクリメントされたCheck Out回数をローカルストレージ３２におけるUsage Ruleにセキュアライトする。その後、ステップＳ５６においてUsage RuleにおけるCheck Out回数のベリファイを行い、ステップＳ５７においてUsage RuleにCheck Out回数が正常に書き込まれたか否かを判定する。正常に書き込まれたなら、ステップＳ４２～ステップＳ４５からなるループ処理に移行する。

【０１２４】操作者からチェックインが要求されたなら、ステップＳ４４がYesとなり、ステップＳ１０１において、既にトラックが記録されているSDメモリカードから、SDメモリカードに固有なMedia-IDと、トラックに固有なContent_IDとを読み取る。ステップＳ１０２では、読み取られたMedia-IDとContent_IDとの組みと、チェックアウト履歴情報におけるMedia-IDとContent_IDとの組みとを照合し、ステップＳ１０３においてSDメモリカード１００に記録されているトラックが、過去にチェックアウトされたものと同一であるか否かを判定する。もし両者が一致である場合（過去にチェックアウトされたものと同一である場合）、ステップＳ５８に移行するが、両者が不一致である場合（過去にチェックアウトされたものでない場合）、チェックイン処理を行わずにステップＳ４２～ステップＳ４５の処理に移行する。

【０１２５】ステップＳ５８では、ローカルストレージ３２のプロテクト領域におけるUsage Ruleをセキュアリードして、ライブラリィ管理部３７はステップＳ５９においてUsage RuleにおけるCheck Out回数が"0"か否かを判定する。Check Out回数が"0"ならば、ステップＳ６０においてトラックを構成するデータセットのうち、Usage Rule以外のものを、チェックインを行うべき記録媒体から読み出し、ローカルストレージ３２に蓄積した後、ステップＳ９２に移行する。Check Out回数が"1"以上なら、そのままステップＳ６６に移行する。ステップＳ９２では、トラックを構成するデータセットを他の記録媒体から削除する。ステップＳ６１では、Check Out回数をインクリメントして、ステップＳ６２においてCheck Out回数が最大数Maxか否かを判定する。Check Out回数がMaxなら、ステップＳ４２～ステップＳ４５からなるループ処理に移行し、Check Out回数がMaxでないなら、ライブラリィ管理部３７はステップＳ６３においてCheck Out回数をセキュアライトし、ステップＳ６４においてCheck Out回数をベリファイする。ステップＳ６５では、セキュアライトが正常に行われたかの判定を行い、セキュアライトされたCheck Out回数が正常ならば、ステップＳ４２～ステップＳ４５からなるループ処理に移行する。

【０１２６】以上説明したように本実施形態によれば、KIOSK端末にて記録された著作物の複製物の記録管理がパソコン上で可能となるので、正当な料金を支払って、KIOSK端末から著作物を購入したユーザは、その著作物についてのチェックアウト チェックインを自分が所有するパソコンに行わせることができる。

（第２実施形態）第２実施形態は、著作物の試聴(プレビュー)を行わせるよう、著作物をセキュアに格納したSDメモリカード１００についての改良に関する。図４２は、第２実施形態に係るプロテクト領域と、ユーザデータ領域のディレクトリ構成を示す図である。本図と、図１２に示したディレクトリ構成とを比較して新規なのは、プロテクト領域及びユーザデータ領域におけるSD_Audioディレクトリのサブディレクトリとして、SD_ADPRVディレクトリィが設けられている点である。ユーザデータ領域におけるSD_ADPRVディレクトリィには、プレビュー用に設けられた『SD_ADPRV.PLM』、『SD_ADPRV.TKM』、『P_AOBxxx.SA1』、『P_POBxxx.JPG/SP1』が配置されている。『SD_ADPRV.PLM』、『SD_ADPRV.TKM』は、配置されているディレクトリが異なるだけで、そのデータ構造は、SD-Audio規格におけるSD_AUDIO.PLM、SD_AUDIO.TKMと全く同一である。P_AOBxxx.SA1、P_POBxxx.JPG/SP1は、配置されているディレクトリと暗号化に用いられた暗号鍵とが異なるが、SD-Audio規格におけるAOBxxx.SA1,POBxxx.SP1/JPGと同一である。

【０１２７】プロテクト領域におけるSD_ADPRVディレクトリィには、『P_AOBSA1.KEY』、『P_POBSP1.KEY』が配置されている。P_AOBSA1.KEYには、複数のExtended Title Key Entryが含まれている。これらのExtended Title Key Entryのデータ構造を図４３に示す。本図において、一部のデータ構成はTitle Key Entryと同一であるが、プレビュー用のフィールドが新たに追加されている点が異なる。図４３のExtended Title Key Entryのフォーマットにおいて、プレビュー用のフィールドには、『Trigger Bit』『Preview Counter』『Preview Threshold』『Check-Valueフィールド』が存在する。

【０１２８】『Trigger Bit』は、Usage RuleにおけるTrigger Bitと同様の趣旨で設けられたフラグであり、"0"に設定されれば、Preview Counter及びPreview Thresholdの組みを参照することにより、プレビューの可否を判定して良い旨を示し、"1"に設定されれば、Preview Counter及びPreview Thresholdの組みだけでなく、他の情報を参照することにより、プレビューの可否を判定す

べき旨を示す。

【０１２９】『Preview Counter』は、1～255の範囲でプレビューの許可回数を示すフィールドであり、図１１に示したDefault OfferのDRMにおけるPlayback Counterに基づき設定される。『Preview Threshold』は、著作物が何秒再生されれば、プレビュー回数を1回とカウントするかを指示するフィールドであり、図１１に示したDefault OfferのDRMにおけるPlayback Timeに基づき設定される。

【０１３０】『Check-Valueフィールド』には、チェック用の文字列パターンが記述される。C_CBCモードによるExtended Title Key Entryの復号が正常に得られた場合、この機器は、本フィールドから文字列パターンを正常に得ることができるが、Extended Title Key Entryの一部が暗号化された状態のまま改竄された場合、このフィールドから文字列パターンを得ることができない。その理由は以下の通りである。

【０１３１】C_CBCモードによる復号は、7バイトのMedia-ID及び部分鍵を用いることにより、8バイトを一単位として行われる。ここでもし、悪意をもったユーザが、暗号化されたままPreview Counter、Preview Thresholdを全く別の値に改竄したとする。そうすると、このPreview Counter、Preview Thresholdを含む8バイトブロックを部分鍵を用いて得られる部分鍵は、予定されていたものとと大きく異なるものが得られる。そうした部分鍵を用いて、後段のブロックを復号してゆくと、最後に文字パターンを含むブロックを復号することにより得られた演算結果は、上述した文字パターンと大きくかけはなれたものとなる。このように、文字パターンは、暗号化されたPreview Threshold、Preview Counterが正常な状態である限り、正常な文字列パターンが復号されることとなるが、Preview Threshold、Preview Counterが改竄されていれば、改竄のAOBファイルを受けて、Check-Valueフィールドにおける文字列パターンは、全くおかしなものとなる。こうした文字列パターンの性質を利用して、Preview Threshold、Preview Counterに対する改竄の有無をチェックすることができる。

【０１３２】続いて、第２実施形態におけるSD-AUDIOプレーヤ１２２～SD-AUDIOプレーヤ１２４の処理について説明する。図４３に示したExtended Title Key Entryを用いて、著作物のプレビューを行う場合、SD-AUDIOプレーヤ１２２～SD-AUDIOプレーヤ１２４に含まれる制御部６４がどのような処理を行うかは、図４４のフローチャートに示されている。以降図４４を参照しながら、第２実施形態における制御部６４の処理について説明する。

【０１３３】制御部６４は、ステップＳ８１においてSDメモリカード１００がカードコネクタ３４に接続されたか否かを判定し、ステップＳ８２においてSDメモリカード１００のSD_ADPRVディレクトリにおけるトラックを一覧表示する。ステップＳ８３においてプレビューすべきトラックの選択待ちを行う。ここで操作者により選択されたトラックをトラック#xとするとステップＳ８４においてトラック#xについてのExtended Title Key Entry #xをプロテクト領域からセキュアリードする。その後、ステップＳ８５において制御部６４は、Trigger Bit#xをチェックする。Trigger Bitが"1"であれば、ステップＳ８６～ステップＳ９７の処理は行わず、処理は終了する。Trigger Bitが"0"であれば、ステップＳ８６において、制御部６４は、Extended Title Key Entry#xに対して、C_CBCモードの復号を行うことにより、文字列パターンを得る。ステップＳ８７において文字列パターンは正常なものかか否かを判定する。異常であれば、処理を終了するが、正常ならば、ステップＳ８８において制御部６４は、Preview Counterが"0"であるか否かを判定する。Preview Counterが"0"であれば処理を終了するが、そうでなければ、制御部６４は、ステップＳ８９において、Extended TitleKey Entry#xにおけるTitle KeyをSDメモリカード１００におけるデ スクランブラ６１に設定する。その後制御部６４は、ステップＳ９０においてトラック#xを再生する。制御部６４は、ステップＳ９１においてPreview Threshold#xに示された時間だけ再生時間が経過するのを待ち、経過すれば、ステップＳ９２においてPreview Counterをデクリメントする。その後、ステップＳ９３においてPreview Counterが1以上であるか0であるかを判定する。1以上であればステップＳ９４においてPreview Counterをセキュアライトし、その後、ステップＳ９５においてPreview Counterをベリファイする。Preview Counterが"0"であれば、ステップＳ９６においてTitleKey Entryを削除し、ステップＳ９７においてAvailability Flagに"0"を設定する。

【０１３４】以上のように本実施形態によれば、Preview Counter、Preview Thresholdは、プロテクト領域に記録されており、改竄は非常に困難となるので、著作物についての著作権を正当に保護しながなら、著作物の試聴を操作者に行わせることができる。以上、2つの実施形態に示される配信システムを運用した場合、著作物の販売は、音楽会社が運営する配信サーバー１０３と、自動販売機、携帯電話機、STBとの間で行われるので、著作物の販売にあたっての流通コストや在庫管理が大きく軽減されることとなる。また、パソコンを所持していないユーザであっても、販売店まで足を運ばずに、携帯電話機やSTBを介して著作物を購入することができ、価格の低下が期待できるなどメリットも大きいため、既存の流通経路を大きく改良できる。これらの点において、本発明に係る配信システム、受信装置、半導体メモリカードは高い産業上の利用可能性を有する。

【０１３５】尚、これらの実施形態は、現状において最善の効果が期待できる形態を記述したものであって、上記実施の形態に限定されるものではない。具体的には、下記のような変更実施が可能である。

(a)第１、第２実施形態における、SDメモリカードは、ユーザデータ領域と、プロテクト領域を備えたが、これに限定されるものではなく、すべてプロテクト領域として実現してもよい。記録媒体としてSDメモリカード１００を使用したが、このような半導体メモリに限定されるものではなく、プロテクト領域を備えていれば、光ディスク、HD等に置き換えることが可能である。

【０１３６】(b)第１、第２実施形態では、1個の著作物はパッケージに対応し、音楽アルバム等、著作物の集合体は、タイトルに対応したが、著作物の集合体を1個のパッケージにて送信してもよい。

(c)トラックのプレビューを行うための条件として、日付による制限（ある期日までは試聴可能）、試聴日数による制限（特定の時間、日数の間は試聴可能）、試聴範囲の制限（トラックの特定の部分のみ試聴可能）、という条件を採用したり、あるいは、これらの組み合わせを採用してもよい。

【０１３７】(d)第１、第２実施形態では、記録再生の対象となるデータを音楽データ、および静止画に限定して説明を行ったが、これに限定されるものではない。記録再生の対象となるデータは任意のディジタルデータであり得る。例えば、記録再生の対象となるデータは、動画、テキストデータ、または、これらを組み合わせることによって得られるデータであってもよい。

【０１３８】(e)第１実施形態においてデジタルターミナルは、DRM中のMove制御情報を参照し、DRMに忠実に、Usage RuleのMove制御情報に設定していたが、デジタルターミナルは、他の情報を参照して、他の基準にてMove制御情報を設定してもよい。例えば、著作物のヒットチャートにおけるランクや、著作物が新譜であるか否か、著作物の売り上げ高等の情報を勘案して、Move制御情報を設定してもよい。

【０１３９】(f)ローカルストレージに書き込まれた暗号化データ、プレーンデータ、暗号鍵、権利証をローカルストレージから読み出し、権利証において移動許可回数に示される回数が0(ゼロ)であるか、1以上であるかを判定を行なって、回数が1以上なら、これらをSDメモリカード１００に再度記録してもよい。

(g)第１実施形態では、SDメモリカード１００に移動許可回数が”1”又は”0”に設定されることを想定していたが、これ以上の移動許可回数を設定してよいことはいうまでもない。配信サーバー１０３により”移動許可回数=6回”と移動制御情報が設定された場合には、移動制御情報に示される移動許可回数は図４５のように更新されながら、権利証は各記録媒体間を移動してゆくこととなる。

【０１４０】

【発明の効果】以上説明したように、本発明に係る配信システムは、第１受信装置、第２受信装置を含み、前記第１受信装置は、コンテンツと、記録媒体に対する当該コンテンツについての複製を管理する管理情報との組みであるデータセットをネットワークを介して配信サーバから受信して、保持する第１受信手段と、前記データセットを他の受信装置に移動することを許可するか否かを示す許可情報を生成し、当該許可情報と、データセットに含まれる管理情報とを含むユーセージルール情報を、データセットに含まれるコンテンツに対応づけて配布媒体に記録する記録手段とを備え、前記第２受信装置は、前記データセットをネットワークを介して配信サーバから受信して、保持する第２受信手段と、前記配布媒体から許可情報を読み出し、読み出された許可情報に、データセットの移動を許可する旨が示されている場合のみ、前記配布媒体から装置内部へのデータセットの移動を行い、データセットを保持するデータセット移動手段と、第２受信手段及びデータセット移動手段の何れか一方によりデータセットが保持された場合、保持されているデータセットにおける管理情報に基づき、同データセットにおけるコンテンツの複製物を生成して記録媒体に記録するチェックアウト手段とを備えており、1つの機器から2つの受信装置へとコンテンツとユーセージルールとの組みを移動させるので、第１受信装置（上述の例でいえばKIOSK端末）にて半導体メモリカードに記録されたコンテンツとユーセージルールとの組みの記録管理を第２受信装置（上述の例でいえばパソコン）に行わせることができる。KIOSK端末にて記録された著作物の複製物の記録管理がパソコン上で可能となるので、正当な料金を支払って、KIOSK端末から著作物を購入したユーザは、その著作物についてのチェックアウト チェックインを自分が所有するパソコンに行わせることができる。

【０１４１】ここで前記チェックアウト手段は、前記記録媒体と接続する接続手段を有していて、当該接続手段に接続された記録媒体に未だコンテンツの複製物が記録されておらず、前記第２受信手段、又は、前記データセット移動手段に保持されている管理情報が、1以上の残り回数を示している場合、データセット移動手段が保持しているデータセットにおけるコンテンツの複製物を記録媒体に記録するものであり、前記第２受信装置は更に、接続手段に接続された記録媒体に既にコンテンツの複製物が記録されている場合、接続手段に接続された記録媒体に記録されているコンテンツの複製物を削除するチェックイン手段と、記録媒体に複製物が記録されれば、チェックアウトの残り回数をデクリメントするよう第２受信手段と、又は、データセット移動手段に保持されている管理情報を更新し、記録媒体におけるコンテンツの複製物が削除されればチェックアウトの残り回数をインクリメントするよう管理情報を更新する更新手段とを備えていてもよい。

【０１４２】この配信システムによれば、第２受信装置によるチェックアウトは、管理情報に示される回数だけ可能なので、著作権者が定めた限度以上のチェックアウ

トが行われることはない。これにより、著作権者の利益が不当に害されることはない。ここで前記チェックアウト手段は、保持しているコンテンツに、固有の識別子を割り当てて、記録媒体に記録する割当部と、接続手段に接続された記録媒体に固有な識別子を記録媒体から読み出し、これと、割当部により割り当てられたコンテンツの識別子との組みを記憶する記憶部とを備え、チェックイン手段は既にコンテンツの複製物が記録されている記録媒体が接続手段に接続されたなら、当該記録媒体に固有な識別子と、コンテンツに固有な識別子との組みを読み取る読取部と、読取部により読み取られた識別子の組みと、記憶部が記憶している識別子の組みとを比較することにより、接続手段に接続された記録媒体に記録されている複製物が、過去に自装置が記録したものと同一であるか否かを判定する比較部と、過去に自装置が記録したものと同一である場合、接続手段に接続された記録媒体に記録されている複製物を読み出して保持し、その後、記録媒体から複製物を削除する保持部とを備えていてもよい。この配信システムによれば、第２受信装置がチェックインを行う場合、記録媒体の識別子及びコンテンツの識別子の組みを照合することにより、過去に自身がチェックアウトしたものか否かを判定し、過去に自身がチェックアウトした複製物のみをチェックインするので、『他の機器がチェックアウトしたコンテンツをチェックインしない』という原則が、ないがしろにされることはない。

【図面の簡単な説明】

【図１】著作物のデータ構造を示す図である。

【図２】（ａ）暗号鍵、権利証抜きで著作物が記録媒体に記録された態様(1)を示す図である。

（ｂ）権利証抜きで著作物が記録媒体に記録された態様(2)を示す図である。

（ｃ）権利証を含んだ状態で著作物が記録媒体に記録された態様(3)を示す図である。

【図３】（ａ）SDメモリカードの外観形状を示す図である。

（ｂ）SDメモリカード１００の階層構造を示す図である。

（ｃ）SDメモリカード１００における物理層の構成を示す図である。

【図４】（ａ）プロテクト領域に暗号鍵のみが格納された状態で非対応機器がSDメモリカード１００に接続された場合を表す図である。

（ｂ）プロテクト領域に暗号鍵のみが格納された状態で対応機器がSDメモリカード１００と接続された場合を表す図である。

（ｃ）プロテクト領域に権利証及び暗号鍵が格納された状態で対応機器が接続され、権利証が、移動を許可する旨の移動制御情報を含んでいる場合を表す図である。

（ｄ）プロテクト領域に権利証及び暗号鍵が格納された状態で対応機器が接続され、権利証に含まれる移動許可回数が0回の場合を示す図である。

【図５】駅構内、店頭にKIOSK端末が設置されている様子を示す図である。

【図６】（ａ）携帯電話機タイプのデジタルターミナル１０９により、著作物を構成する暗号化データ、プレーンデータ、暗号鍵、権利証がSDメモリカード１００に書き込まれる様子を示す図である。

（ｂ）STBタイプのデジタルターミナル１１０により、著作物を構成する暗号化データ、プレーンデータ、暗号鍵、権利証がSDメモリカード１００に書き込まれる様子を示す図である。

【図７】（ａ）様々なタイプのカスタマーズデバイスを示す図である。

（ｂ）様々なタイプのSD-AUDIOプレーヤを示す図である。

【図８】（ａ）ネットワークに接続された配信サーバー１０３と、複数のユーザが所有するカスタマーズデバイス（パソコン１１１～１１６）とを示す図である。

（ｂ）（ｃ）3回という範囲でカスタマーズデバイス１１１がチェックアウト チェックインを行う様子を示す図である。

【図９】本実施形態に係る配信システムに含まれる配信サーバと、複数の機器と、再生装置とを示す図である。

【図１０】流通時における著作物データのタイトル及びパッケージのデータ構造を示した図である。

【図１１】Default Offerのデータ構造を階層的に示す図である。

【図１２】著作物のデータセットを記録するために形成されるファイル、ディレクトリを示す図である。

【図１３】AOBファイルのデータ構成を階層的に示す図である。

【図１４】AOBファイルに収録されている各AOB、AOB_BLOCKが連続して再生されることにより、どのような再生内容が再生されるかを示す。

【図１５】図１４に示したタイトル（音楽アルバム）を格納した8つのAOBファイルを示す図である。

【図１６】（ａ）Track Managerの構成を段階的に詳細化した図である。

（ｂ）TKGIの詳細構成を示す図である。

【図１７】TKIと、図１４に示したAOBファイル及びAOBとの相互関係を示す図である。

【図１８】（ａ）（ｂ）2つのトラックを1つに統合する場合にTKIがどのように設定されるかを示す図である。

【図１９】（ａ）（ｂ）1つのトラックを2つのトラックに分割する場合を想定した図である。

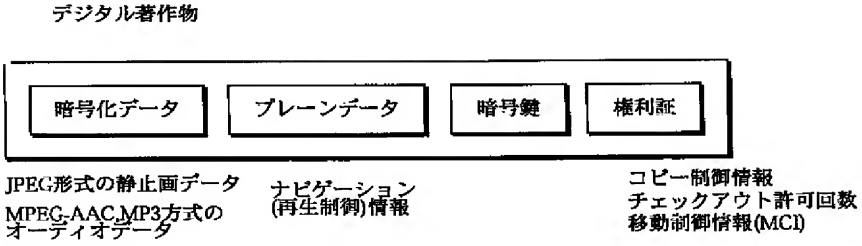
【図２０】AOB_ELEMENT#1～#4からなるAOBが格納されているクラスタ007～クラスタ00Eを示す図である。

【図２１】Track Managerに含まれるTKI#2～TKI#4についてのTKI_POB_SRPの設定例を示す図である。

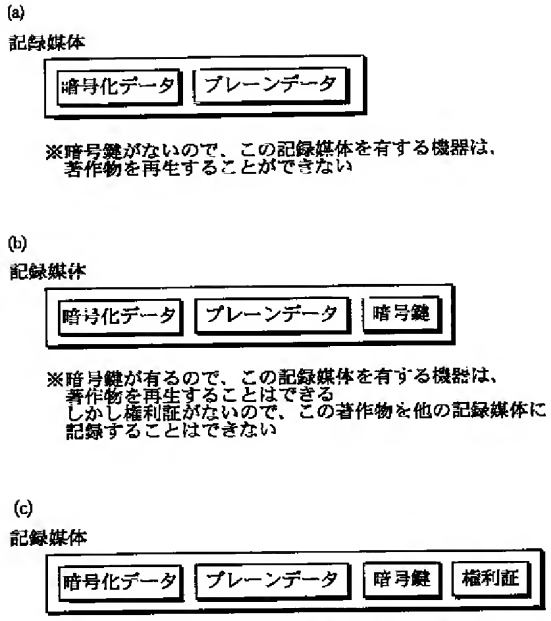
【図２２】Default_Playlist情報、TKI、AOBファイルの相互関係を示す図である。
【図２３】（ａ）（ｂ）トラックの順序を入れ替える場合を想定した図である。
【図２４】『STKIxxx.SDT』の内部構成を示す図である。
【図２５】SD_Audioディレクトリに含まれる3つのAOB#1、AOB#2、AOB#3、2つのPOB001.SP1、POB002.SP1がSD_ADEXTディレクトリィに含まれる3つのSTKI001.SDT、STKI002.SDT、STKI003.SDTとどのように対応するかを示す図である。
【図２６】AOBSA1.URMの構成を示す図である。
【図２７】SD_Audioディレクトリの下にAOBファイルが8つ存在し、これらに対応する暗号鍵がAOBSA1.KEYに8つ収録され、これらに対応するUsage RuleがAOBSA1.URMに8つ収録されている場合、AOBSA1.KEYと、AOBSA1.URMと、AOBファイルとの対応を示す図である。
【図２８】（ａ）（ｂ）AOBSA1.KEY、AOBSA1.URMと、AOBファイルとの対応関係を示す図である。
【図２９】Title Key Entryの内部構成を示す図である。
【図３０】（ａ）（ｂ）SDメモリカード１００におけるユーザデータ領域のオーディオオブジェクトを全てローカルストレージに移動させるケースを想定した図である。
【図３１】（ａ）（ｂ）ユーザデータ領域における8つのオーディオオブジェクトのうち、3つのみを移動させようとする場合、SDメモリカード１００のユーザデータ領域にどのようなファイルが配置されるかを示す図である。
【図３２】図２５に示したAOBファイル、POBファイル、STKIファイルがSDメモリカード１００からローカルストレージへとどのように移動するかを示す図である。
【図３３】デジタルターミナルの構成を示す図である。
【図３４】（ａ）カスタマーズデバイスの構成を示す図である。
（ｂ）SD-Audioプレーヤ１２２～１２４の内部構成を示す図である。
【図３５】デジタルターミナルにおけるセキュア処理部２６の内部構成を示す図である。
【図３６】カスタマーズデバイスにおけるセキュア処理部３８の内部構成を示す図である。
【図３７】販売サービス制御部２７の処理手順を記載したフローチャートである。
【図３８】販売サービス制御部２７の処理手順を記載したフローチャートである。
【図３９】ライブラリィ管理部３７の処理手順を記載したフローチャートである。
【図４０】ライブラリィ管理部３７の処理手順を記載したフローチャートである。
【図４１】ライブラリィ管理部３７の処理手順を記載したフローチャートである。
【図４２】第２実施形態に係るプロテクト領域と、ユーザデータ領域のディレクトリ構成を示す図である。
【図４３】P_AOBSA1.KEYに含まれるExtended Title Key Entryのデータ構造を示す図である。
【図４４】プレビューを行う場合のライブラリィ管理部３７の処理内容を示すフローチャートである。
【図４５】移動許可回数が6回に設定された場合に、移動許可回数が更新される様子を示す図である。
【符号の説明】
１　システム領域
２　Hidden領域
３　プロテクト領域
４　AKE処理部
５　AKE処理部
６　KS復号化部
７　KS暗号化部
８　ユーザデータ領域
２１　リリースコンテンツブラウザ部
２２　タッチパネル
２３　通信部
２４　カードコネクタ
２５　課金部
２６　セキュア処理部
２７　販売サービス制御部
３２　ローカルストレージ
３３　通信部
３４　カードコネクタ
３５　ホームライブラリィブラウザ部
３６　入力受付部
３７　ライブラリィ管理部
３８　セキュア処理部
３９　再生部
４１　MKB処理部
４２　ID処理部
４３　AKE処理部
４４　Kmu暗号化部
４５　STI暗号化部
４６　Ks暗号化部
５１　MKB処理部
５２　ID処理部
５３　AKE処理部
５４　Ks復号化部
５５　Kmu復号化部
５６　STI復号化部
６０　カードコネクタ
６１　デ スクランブラ
６２　AACデコーダ
６３　A/Dコンバータ

１００　SDメモリカード
１０１　プロテクトスイッチ
１０３　配信サーバ
１０４～１０８　KIOSK端末
１０９　携帯電話機
１１０　STB
１１１～１２１　カースタマーズデバイス
１２２～１２４　SD-Audioプレーヤ

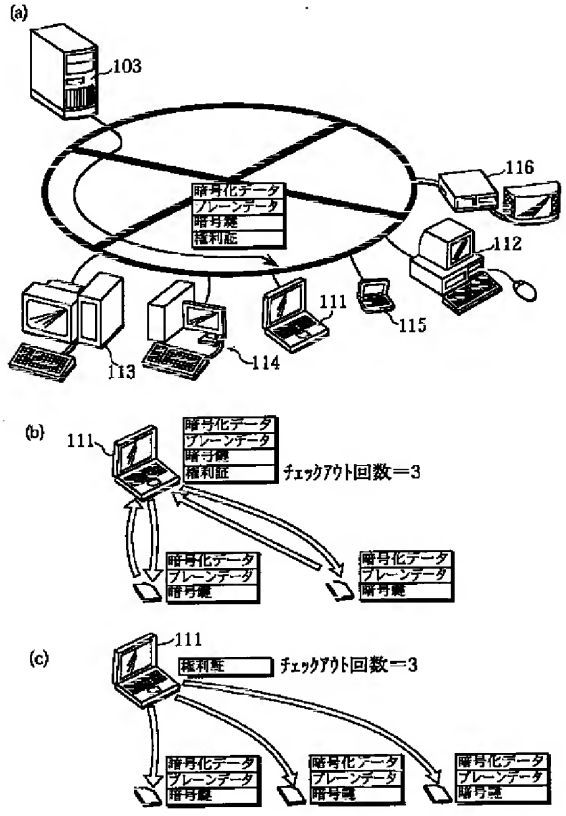
【図１】



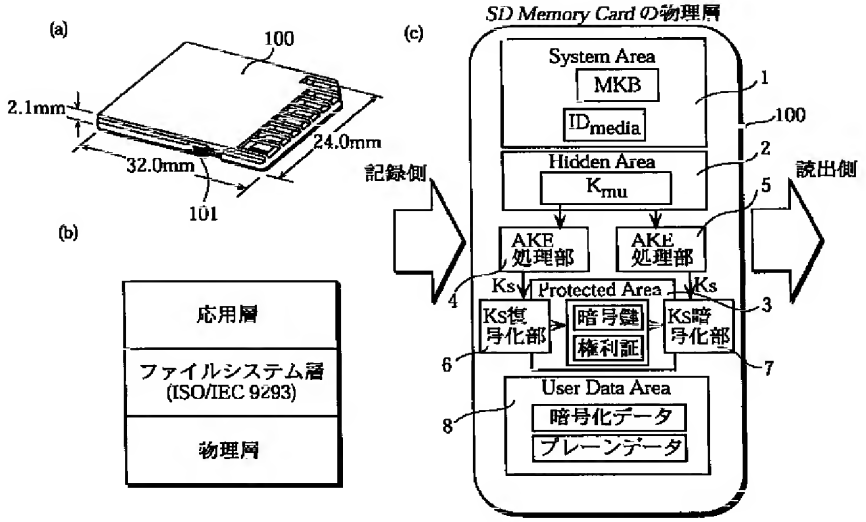
【図２】



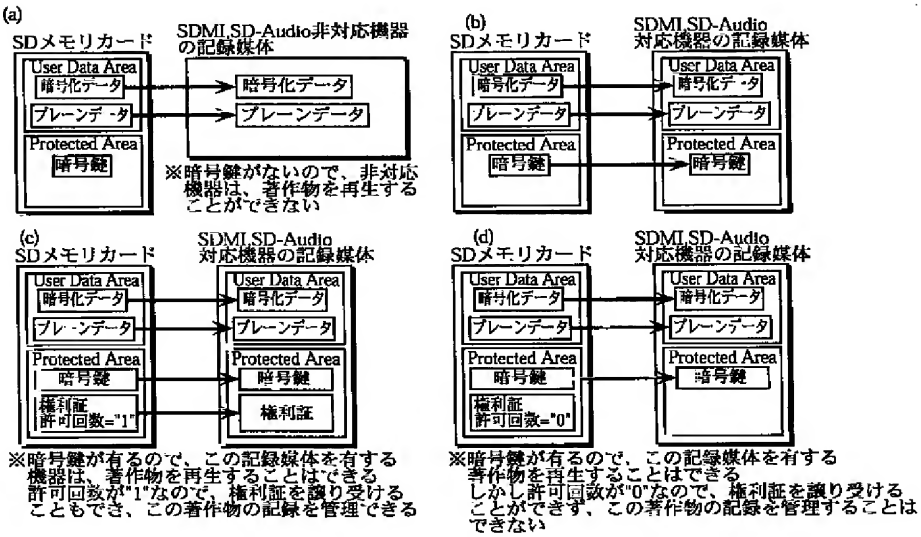
【図８】



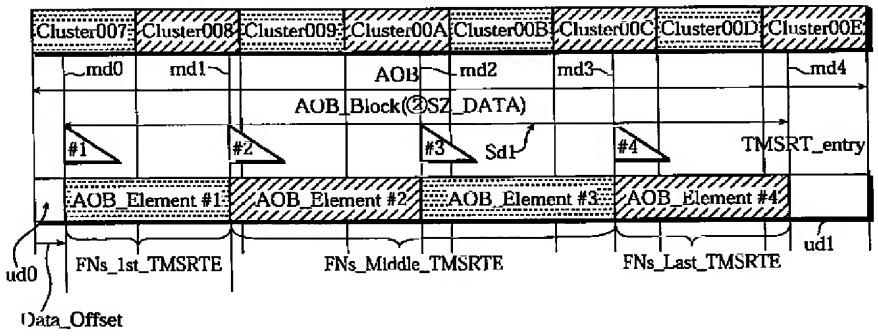
【図３】


(a)
100
2.1mm
24.0mm
32.0mm
101
(b)
応用層
ファイルシステム層
(ISO/IEC 9293)
物理層
(c)
SD Memory Card の物理層
System Area
MKB
IDmedia
1
100
Hidden Area
Kmu
2
記録側
読出側
5
AKE
処理部
AKE
処理部
Ks
Protected Area
Ks
4
3
KS複
号化部
暗号鍵
権利証
KS暗
号化部
6
7
User Data Area
暗号化データ
プレーンデータ
8

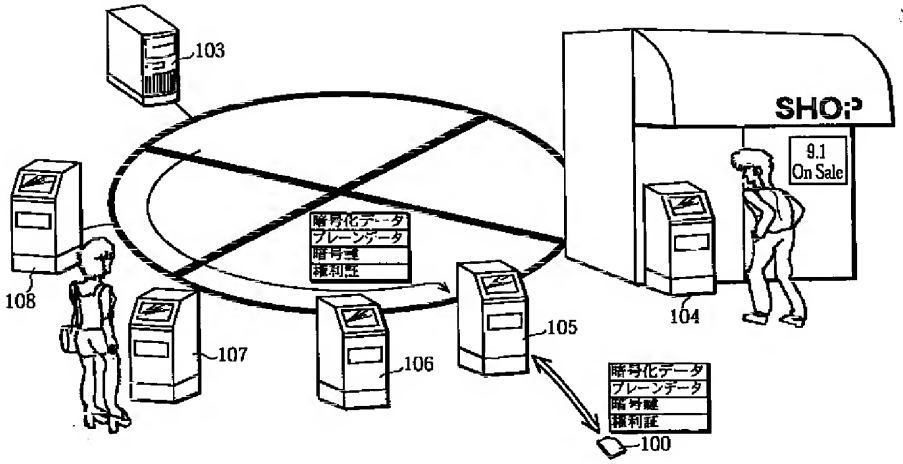
【図４】


(a)
SDメモリカード
SDMI,SD-Audio非対応機器
の記録媒体
User Data Area
暗号化データ
プレーンデータ
Protected Area
暗号鍵
暗号化データ
プレーンデータ
※暗号鍵がないので、非対応
機器は、著作物を再生する
ことができない
(b)
SDメモリカード
SDMI,SD-Audio
対応機器の記録媒体
(c)
SDメモリカード
SDMI,SD-Audio
対応機器の記録媒体
権利証
許可回数="1"
権利証
※暗号鍵が有るので、この記録媒体を有する
機器は、著作物を再生することはできる
許可回数が"1"なので、権利証を譲り受ける
こともでき、この著作物の記録を管理できる
(d)
SDメモリカード
SDMI,SD-Audio
対応機器の記録媒体
権利証
許可回数="0"
※暗号鍵が有るので、この記録媒体を有する
著作物を再生することはできる
しかし許可回数が"0"なので、権利証を譲り受ける
ことができず、この著作物の記録を管理することは
できない

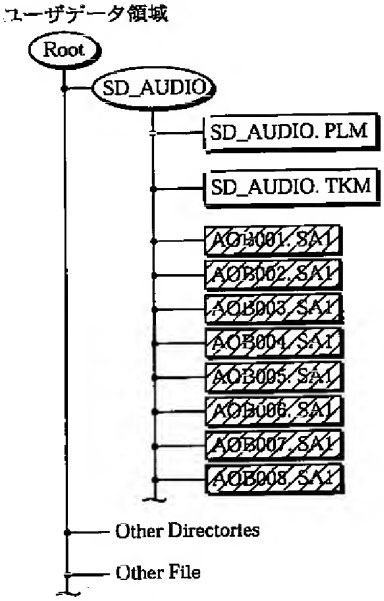
【図２０】


Cluster007
Cluster008
Cluster009
Cluster00A
Cluster00B
Cluster00C
Cluster00D
Cluster00E
md0
md1
AOB
md2
md3
md4
AOB_Block(②SZ_DATA)
#1
#2
#3
Sd1
#4
TMSRT_entry
AOB_Element #1
AOB_Element #2
AOB_Element #3
AOB_Element #4
ud0
ud1
FNs_1st_TMSRTE
FNs_Middle_TMSRTE
FNs_Last_TMSRTE
Data_Offset

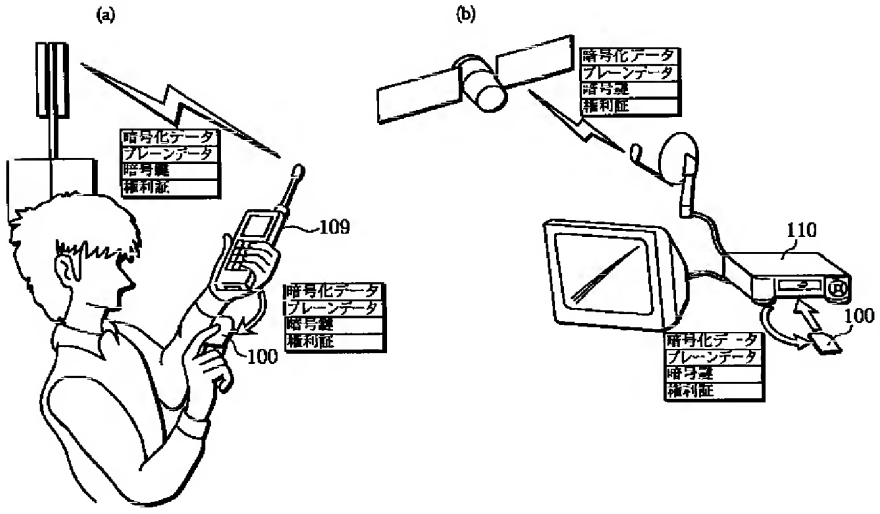
【図５】


103
SHOP
9.1
On Sale
暗号化データ
プレーンデータ
暗号鍵
権利証
108
107
106
105
104
100

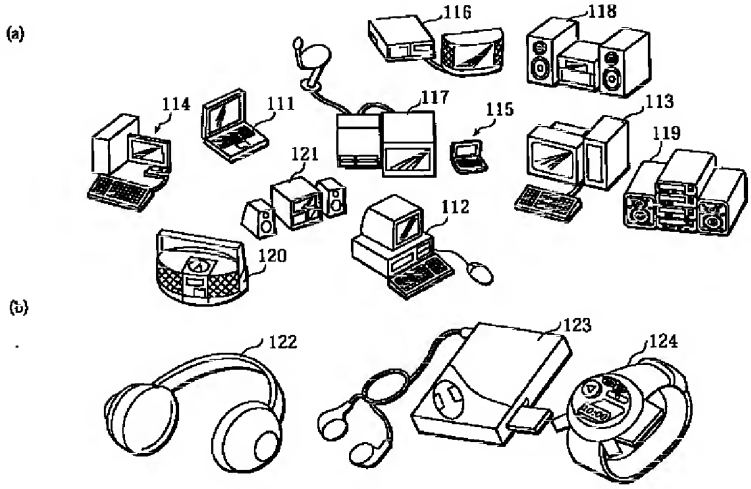
【図１５】


ユーザデータ領域
Root
SD_AUDIO
SD_AUDIO. PLM
SD_AUDIO. TKM
AOB001. SA1
AOB002. SA1
AOB003. SA1
AOB004. SA1
AOB005. SA1
AOB006. SA1
AOB007. SA1
AOB008. SA1
Other Directories
Other File

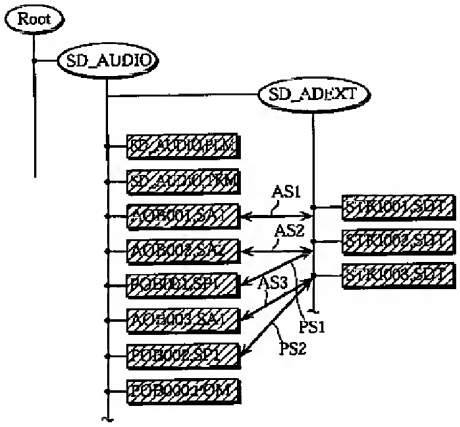
【図６】


(a)
(b)
暗号化データ
プレーンデータ
暗号鍵
権利証
109
100
110

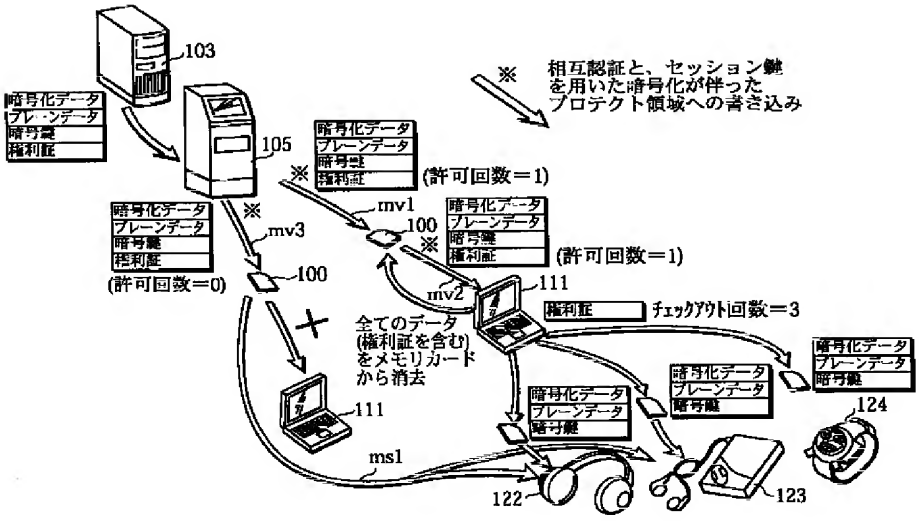
【図7】


(a)
(b)
111
112
113
114
115
116
117
118
119
120
121
122
123
124

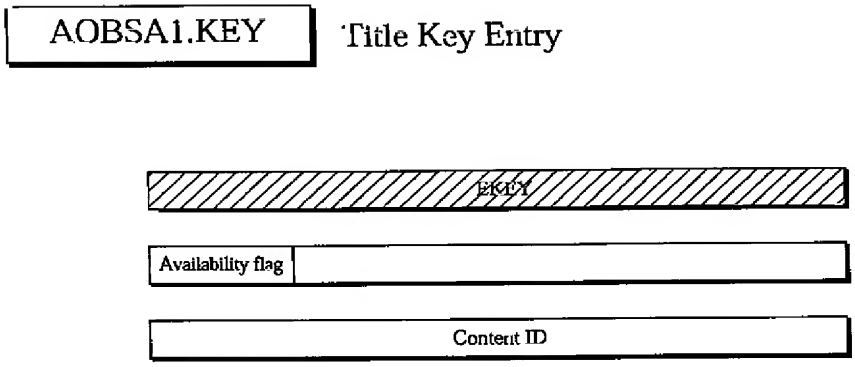
【図25】


Root
SD_AUDIO
SD_ADEXT
AS1
AS2
AS3
PS1
PS2

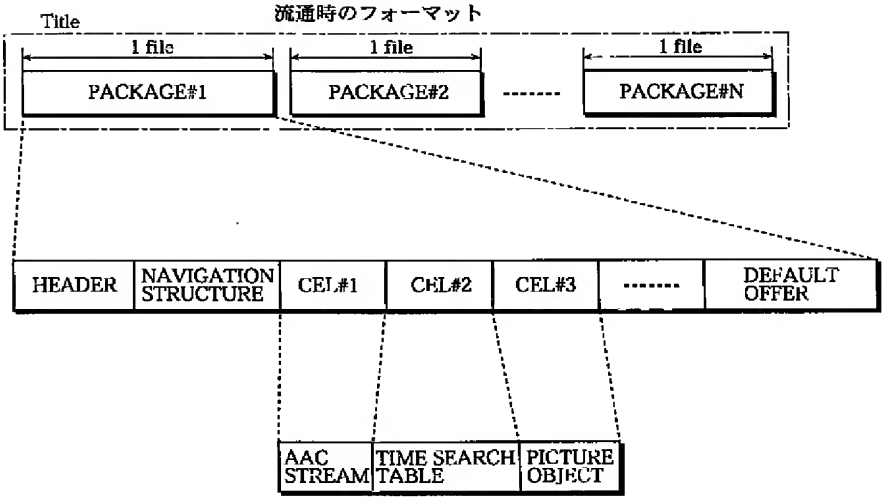
【図9】


※ 相互認証と、セッション鍵を用いた暗号化が伴ったプロテクト領域への書き込み
暗号化データ
プレーンデータ
暗号鍵
権利証
103
105
(許可回数＝1)
(許可回数＝0)
mv1
mv2
mv3
ms1
100
111
122
123
124
チェックアウト回数＝3
全てのデータ(権利証を含む)をメモリカードから消去

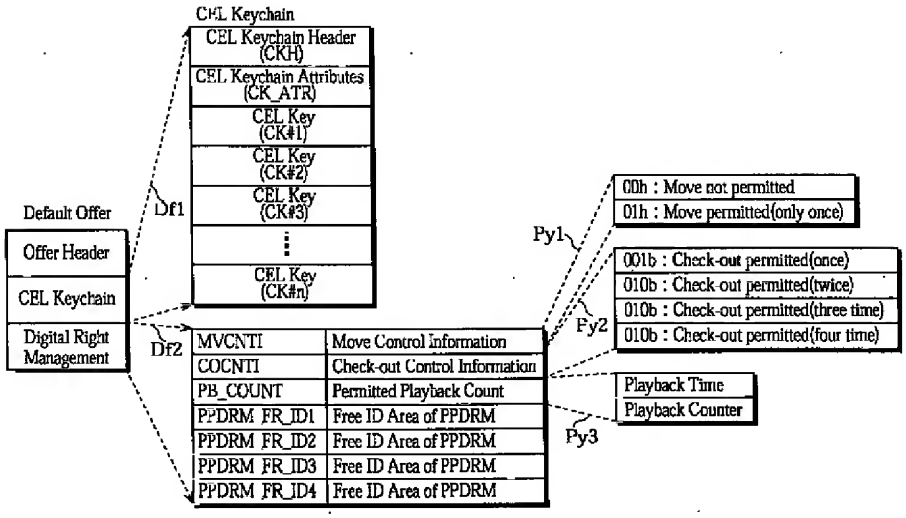
【図29】


AOBSA1.KEY
Title Key Entry
EKEY
Availability flag
Content ID

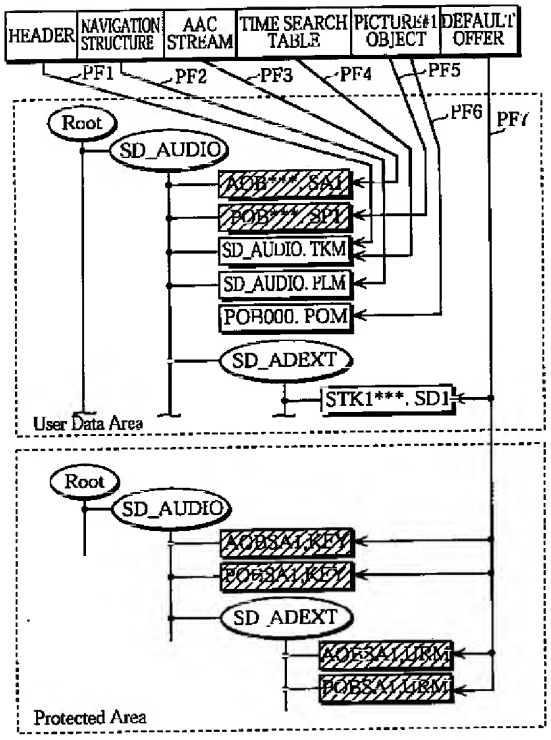
【図１０】


Title
流通時のフォーマット
1 file
1 file
1 file
PACKAGE#1
PACKAGE#2
PACKAGE#N
HEADER
NAVIGATION STRUCTURE
CEL#1
CEL#2
CEL#3
DEFAULT OFFER
AAC STREAM
TIME SEARCH TABLE
PICTURE OBJECT

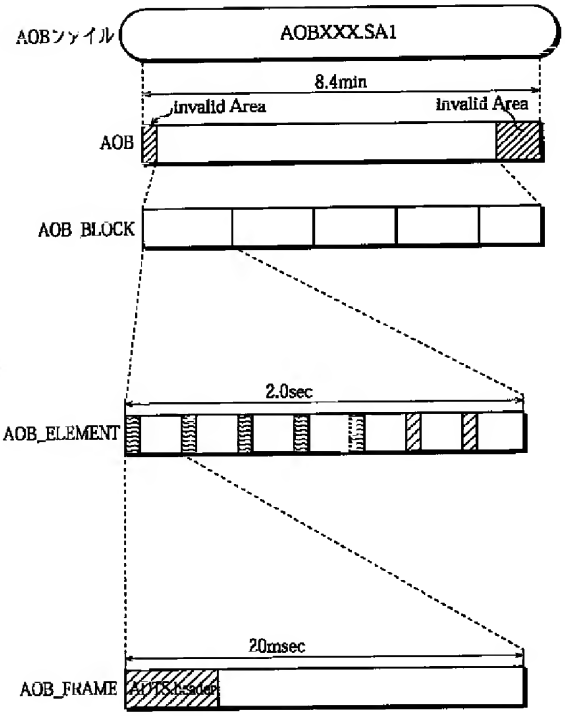
【図１１】


CEL Keychain
CEL Keychain Header (CKH)
CEL Keychain Attributes (CK_ATR)
CEL Key (CK#1)
CEL Key (CK#2)
CEL Key (CK#3)
CEL Key (CK#n)
Default Offer
Offer Header
CEL Keychain
Digital Right Management
Df1
Df2
MVCNTI
Move Control Information
COCNTI
Check-out Control Information
PB_COUNT
Permitted Playback Count
PPDRM_FR_ID1
Free ID Area of PPDRM
PPDRM_FR_ID2
Free ID Area of PPDRM
PPDRM_FR_ID3
Free ID Area of PPDRM
PPDRM_FR_ID4
Free ID Area of PPDRM
Py1
00h : Move not permitted
01h : Move permitted(only once)
Py2
001b : Check-out permitted(once)
010b : Check-out permitted(twice)
010b : Check-out permitted(three time)
010b : Check-out permitted(four time)
Py3
Playback Time
Playback Counter

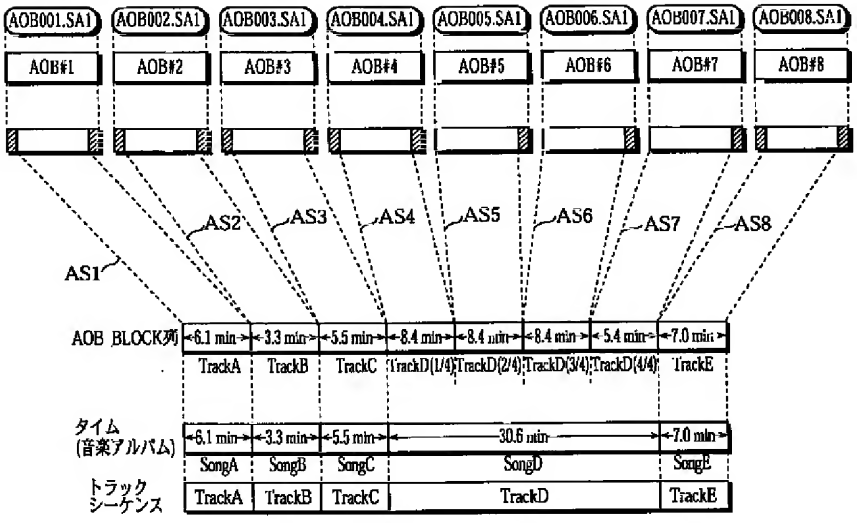
【図１２】


HEADER
NAVIGATION STRUCTURE
AAC STREAM
TIME SEARCH TABLE
PICTURE#1 OBJECT
DEFAULT OFFER
PF1
PF2
PF3
PF4
PF5
PF6
PF7
Root
SD_AUDIO
AOB***. SA1
POB***. SP1
SD_AUDIO. TKM
SD_AUDIO. PLM
POB000. POM
SD_ADEXT
STK1***. SD1
User Data Area
Root
SD_AUDIO
AOBSA1.KD1
POBSA1.KD1
SD_ADEXT
AOBSA1.URM
POBSA1.URM
Protected Area

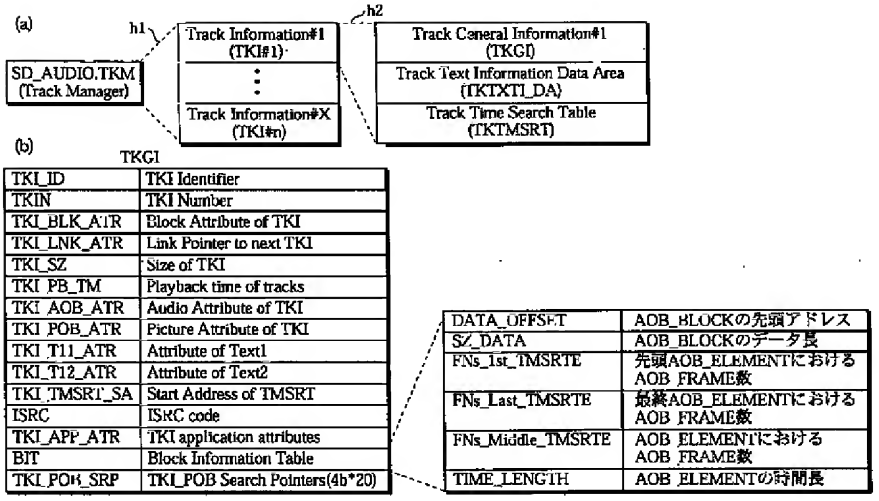
【図１３】


AOBファイル
AOBXXX.SA1
8.4min
Invalid Area
Invalid Area
AOB
AOB BLOCK
2.0sec
AOB_ELEMENT
20msec
AOB_FRAME

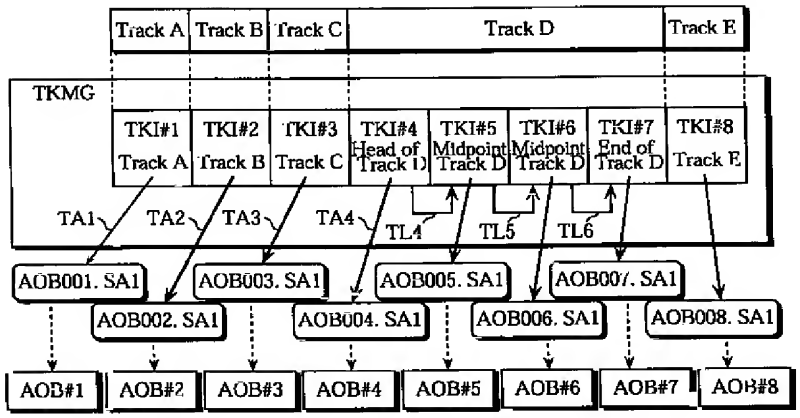
【図１４】


AOB001.SA1
AOB002.SA1
AOB003.SA1
AOB004.SA1
AOB005.SA1
AOB006.SA1
AOB007.SA1
AOB008.SA1
AOB#1
AOB#2
AOB#3
AOB#4
AOB#5
AOB#6
AOB#7
AOB#8
AS1
AS2
AS3
AS4
AS5
AS6
AS7
AS8
AOB BLOCK列
6.1 min
3.3 min
5.5 min
8.4 min
8.4 min
8.4 min
5.4 min
7.0 min
TrackA
TrackB
TrackC
TrackD(1/4)
TrackD(2/4)
TrackD(3/4)
TrackD(4/4)
TrackE
タイム
(音楽アルバム)
6.1 min
3.3 min
5.5 min
30.6 min
7.0 min
SongA
SongB
SongC
SongD
SongE
トラック
シーケンス
TrackA
TrackB
TrackC
TrackD
TrackE

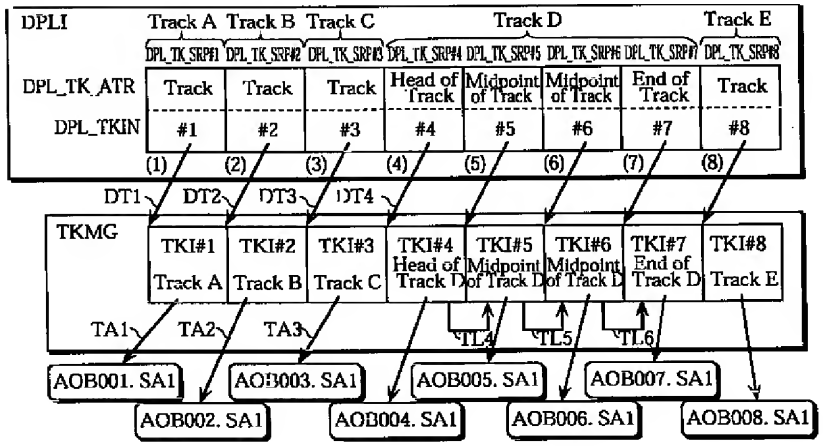
【図１６】


(a)
h1
h2
SD_AUDIO.TKM
(Track Manager)
Track Information#1
(TKI#1)
Track Information#X
(TKI#n)
Track General Information#1
(TKGI)
Track Text Information Data Area
(TKTXTI_DA)
Track Time Search Table
(TKTMSRT)
(b)
TKGI
TKI_ID | TKI Identifier
TKIN | TKI Number
TKI_BLK_ATR | Block Attribute of TKI
TKI_LNK_ATR | Link Pointer to next TKI
TKI_SZ | Size of TKI
TKI_PB_TM | Playback time of tracks
TKI_AOB_ATR | Audio Attribute of TKI
TKI_POB_ATR | Picture Attribute of TKI
TKI_T11_ATR | Attribute of Text1
TKI_T12_ATR | Attribute of Text2
TKI_TMSRT_SA | Start Address of TMSRT
ISRC | ISRC code
TKI_APP_ATR | TKI application attributes
BIT | Block Information Table
TKI_POB_SRP | TKI_POB Search Pointers(4b*20)
DATA_OFFSET | AOB_BLOCKの先頭アドレス
SZ_DATA | AOB_BLOCKのデータ長
FNs_1st_TMSRTE | 先頭AOB_ELEMENTにおけるAOB_FRAME数
FNs_Last_TMSRTE | 最終AOB_ELEMENTにおけるAOB_FRAME数
FNs_Middle_TMSRTE | AOB_ELEMENTにおけるAOB_FRAME数
TIME_LENGTH | AOB_ELEMENTの時間長

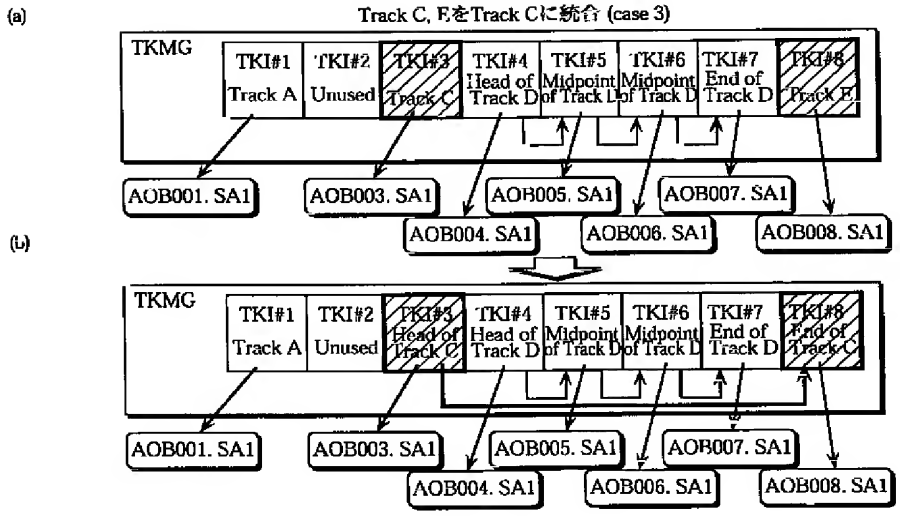
【図１７】


Track A
Track B
Track C
Track D
Track E
TKMG
TKI#1 Track A
TKI#2 Track B
TKI#3 Track C
TKI#4 Head of Track D
TKI#5 Midpoint Track D
TKI#6 Midpoint Track D
TKI#7 End of Track D
TKI#8 Track E
TA1
TA2
TA3
TA4
TL4
TL5
TL6
AOB001. SA1
AOB002. SA1
AOB003. SA1
AOB004. SA1
AOB005. SA1
AOB006. SA1
AOB007. SA1
AOB008. SA1
AOB#1
AOB#2
AOB#3
AOB#4
AOB#5
AOB#6
AOB#7
AOB#8

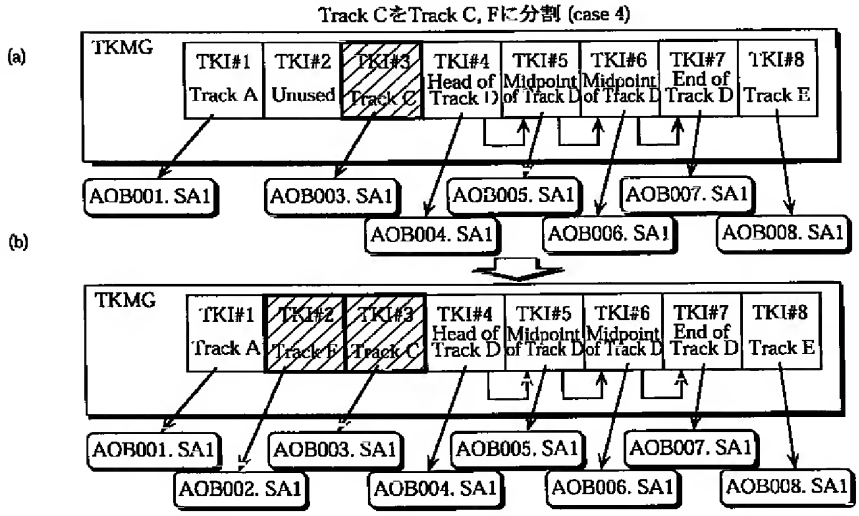
【図２２】


DPLI
Track A
Track B
Track C
Track D
Track E
DPL_TK_SRP#1
DPL_TK_SRP#2
DPL_TK_SRP#3
DPL_TK_SRP#4
DPL_TK_SRP#5
DPL_TK_SRP#6
DPL_TK_SRP#7
DPL_TK_SRP#8
DPL_TK_ATR
Track
Track
Track
Head of Track
Midpoint of Track
Midpoint of Track
End of Track
Track
DPL_TKIN
#1
#2
#3
#4
#5
#6
#7
#8
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
DT1
DT2
DT3
DT4
TKMG
TKI#1 Track A
TKI#2 Track B
TKI#3 Track C
TKI#4 Head of Track D
TKI#5 Midpoint of Track D
TKI#6 Midpoint of Track D
TKI#7 End of Track D
TKI#8 Track E
TA1
TA2
TA3
TL4
TL5
TL6
AOB001. SA1
AOB002. SA1
AOB003. SA1
AOB004. SA1
AOB005. SA1
AOB006. SA1
AOB007. SA1
AOB008. SA1

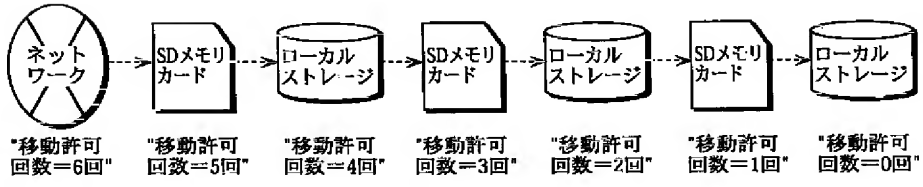
【図１８】


(a)
Track C, FをTrack Cに統合 (case 3)
TKMG
TKI#1 Track A
TKI#2 Unused
TKI#3 Track C
TKI#4 Head of Track D
TKI#5 Midpoint of Track D
TKI#6 Midpoint of Track D
TKI#7 End of Track D
TKI#8 Track F
AOB001. SA1
AOB003. SA1
AOB005. SA1
AOB007. SA1
AOB004. SA1
AOB006. SA1
AOB008. SA1
(b)
TKMG
TKI#1 Track A
TKI#2 Unused
TKI#3 Head of Track C
TKI#4 Head of Track D
TKI#5 Midpoint of Track D
TKI#6 Midpoint of Track D
TKI#7 End of Track D
TKI#8 End of Track C
AOB001. SA1
AOB003. SA1
AOB005. SA1
AOB007. SA1
AOB004. SA1
AOB006. SA1
AOB008. SA1

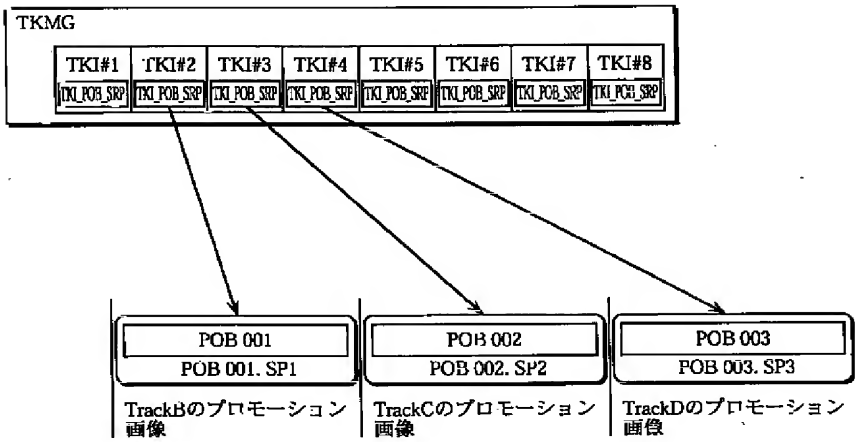
【図１９】


Track CをTrack C, Fに分割 (case 4)
(a)
TKMG
TKI#1 Track A
TKI#2 Unused
TKI#3 Track C
TKI#4 Head of Track D
TKI#5 Midpoint of Track D
TKI#6 Midpoint of Track D
TKI#7 End of Track D
TKI#8 Track E
AOB001. SA1
AOB003. SA1
AOB005. SA1
AOB007. SA1
AOB004. SA1
AOB006. SA1
AOB008. SA1
(b)
TKMG
TKI#1 Track A
TKI#2 Track F
TKI#3 Track C
TKI#4 Head of Track D
TKI#5 Midpoint of Track D
TKI#6 Midpoint of Track D
TKI#7 End of Track D
TKI#8 Track E
AOB001. SA1
AOB003. SA1
AOB005. SA1
AOB007. SA1
AOB002. SA1
AOB004. SA1
AOB006. SA1
AOB008. SA1

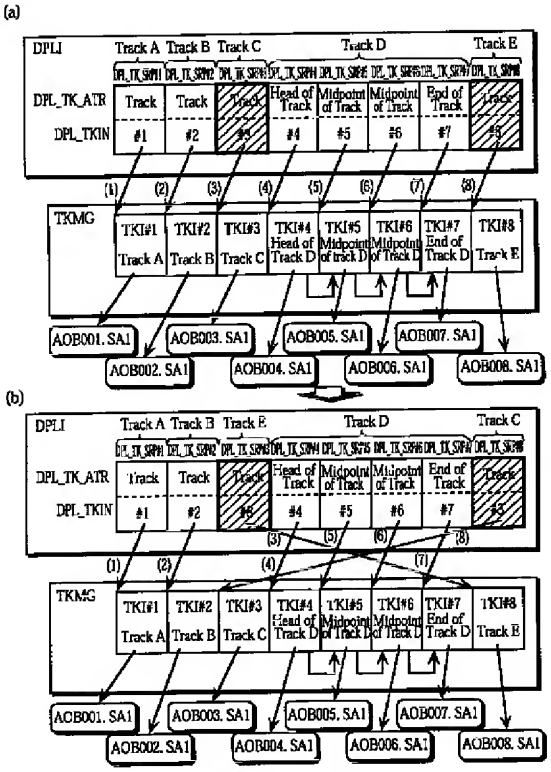
【図４５】


ネットワーク
SDメモリカード
ローカルストレージ
SDメモリカード
ローカルストレージ
SDメモリカード
ローカルストレージ
"移動許可回数＝6回"
"移動許可回数＝5回"
"移動許可回数＝4回"
"移動許可回数＝3回"
"移動許可回数＝2回"
"移動許可回数＝1回"
"移動許可回数＝0回"

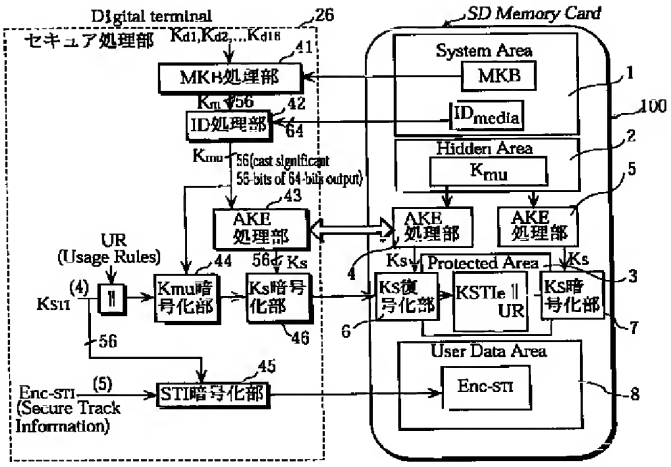
【図２１】


TKMG
TKI#1
TKI#2
TKI#3
TKI#4
TKI#5
TKI#6
TKI#7
TKI#8
TKI_POB_SRP
POB 001
POB 001. SP1
POB 002
POB 002. SP2
POB 003
POB 003. SP3
TrackBのプロモーション画像
TrackCのプロモーション画像
TrackDのプロモーション画像

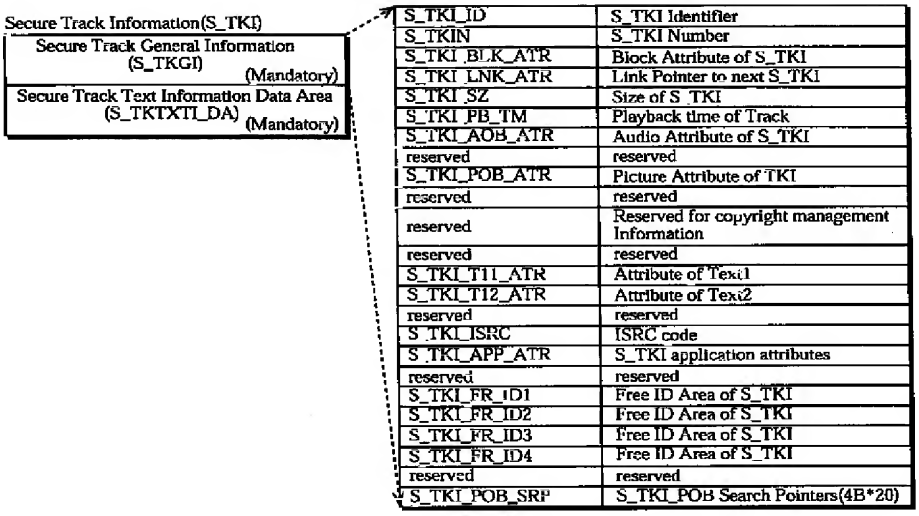
【図２３】


(a)
DPLI
Track A
Track B
Track C
Track D
Track E
DPL_TK_ATR
DPL_TKIN
Track
Head of Track
Midpoint of Track
End of Track
TKMG
TKI#1
TKI#2
TKI#3
TKI#4
TKI#5
TKI#6
TKI#7
TKI#8
AOB001. SA1
AOB002. SA1
AOB003. SA1
AOB004. SA1
AOB005. SA1
AOB006. SA1
AOB007. SA1
AOB008. SA1
(b)

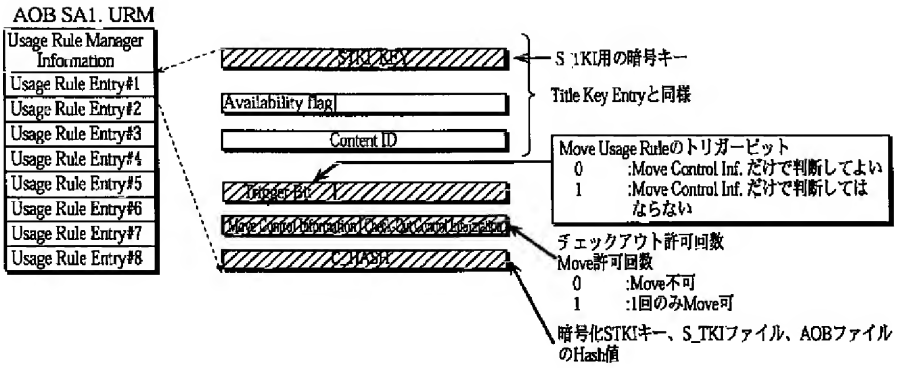
【図３５】


Digital terminal
26
SD Memory Card
セキュア処理部
Kd1,Kd2,...Kd18
41
MKB処理部
Kmu
56
42
ID処理部
64
Kmu
56(cast significant 55-bits of 64-bits output)
43
AKE 処理部
UR (Usage Rules)
44
56
Ks
Ksti
Kmu暗号化部
Ks暗号化部
46
45
Enc-sti
(5)
STI暗号化部
(Secure Track Information)
System Area
MKB
IDmedia
100
1
Hidden Area
Kmu
2
5
AKB 処理部
AKE 処理部
Protected Area
4
3
KS復号化部
KSTIe ‖ UR
KS暗号化部
6
7
User Data Area
Enc-sti
8

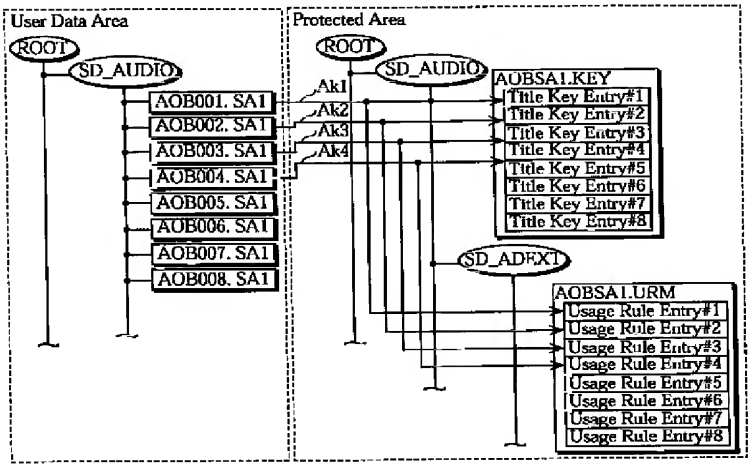
【図24】


Secure Track Information(S_TKI)
Secure Track General Information (S_TKGI) (Mandatory)
Secure Track Text Information Data Area (S_TKTXTI_DA) (Mandatory)
S_TKI_ID | S_TKI Identifier
S_TKIN | S_TKI Number
S_TKI_BLK_ATR | Block Attribute of S_TKI
S_TKI_LNK_ATR | Link Pointer to next S_TKI
S_TKI_SZ | Size of S_TKI
S_TKI_PB_TM | Playback time of Track
S_TKI_AOB_ATR | Audio Attribute of S_TKI
reserved | reserved
S_TKI_POB_ATR | Picture Attribute of TKI
reserved | reserved
reserved | Reserved for copyright management Information
reserved | reserved
S_TKI_T11_ATR | Attribute of Text1
S_TKI_T12_ATR | Attribute of Text2
reserved | reserved
S_TKI_ISRC | ISRC code
S_TKI_APP_ATR | S_TKI application attributes
reserved | reserved
S_TKI_FR_ID1 | Free ID Area of S_TKI
S_TKI_FR_ID2 | Free ID Area of S_TKI
S_TKI_FR_ID3 | Free ID Area of S_TKI
S_TKI_FR_ID4 | Free ID Area of S_TKI
reserved | reserved
S_TKI_POB_SRP | S_TKI_POB Search Pointers(4B*20)

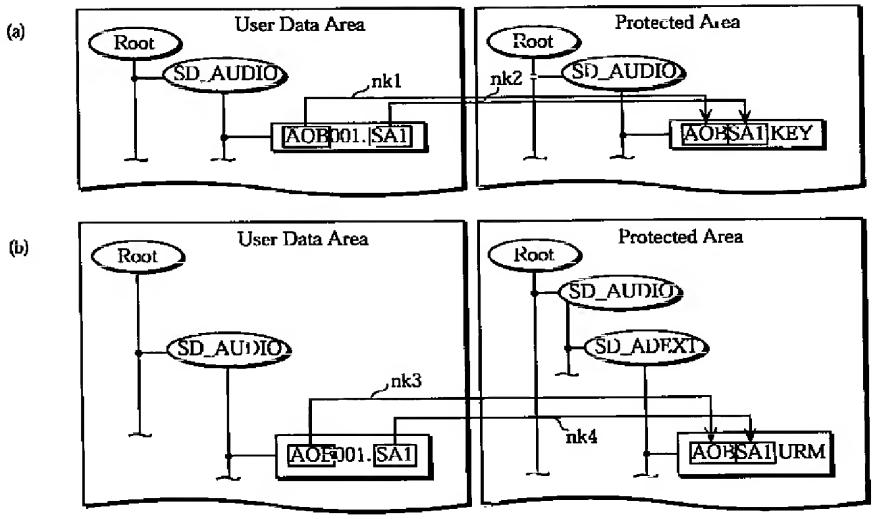
【図26】


AOB SA1. URM
Usage Rule Manager Information
Usage Rule Entry#1
Usage Rule Entry#2
Usage Rule Entry#3
Usage Rule Entry#4
Usage Rule Entry#5
Usage Rule Entry#6
Usage Rule Entry#7
Usage Rule Entry#8
STKI KEY
Availability flag
Content ID
Trigger Bit
Move Control Information Check Out Control Information
S_TKI_HASH
S_TKI用の暗号キー
Title Key Entryと同様
Move Usage Ruleのトリガービット
0 :Move Control Inf. だけで判断してよい
1 :Move Control Inf. だけで判断してはならない
チェックアウト許可回数
Move許可回数
0 :Move不可
1 :1回のみMove可
暗号化STKIキー、S_TKIファイル、AOBファイルのHash値

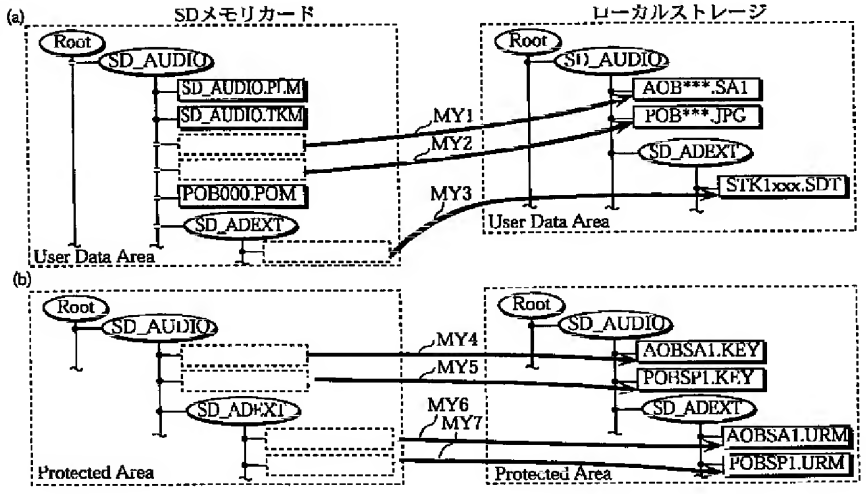
【図27】


User Data Area
ROOT
SD_AUDIO
AOB001. SA1
AOB002. SA1
AOB003. SA1
AOB004. SA1
AOB005. SA1
AOB006. SA1
AOB007. SA1
AOB008. SA1
Protected Area
ROOT
SD_AUDIO
Ak1
Ak2
Ak3
Ak4
AOBSA1.KEY
Title Key Entry#1
Title Key Entry#2
Title Key Entry#3
Title Key Entry#4
Title Key Entry#5
Title Key Entry#6
Title Key Entry#7
Title Key Entry#8
SD_ADEXT
AOBSA1.URM
Usage Rule Entry#1
Usage Rule Entry#2
Usage Rule Entry#3
Usage Rule Entry#4
Usage Rule Entry#5
Usage Rule Entry#6
Usage Rule Entry#7
Usage Rule Entry#8

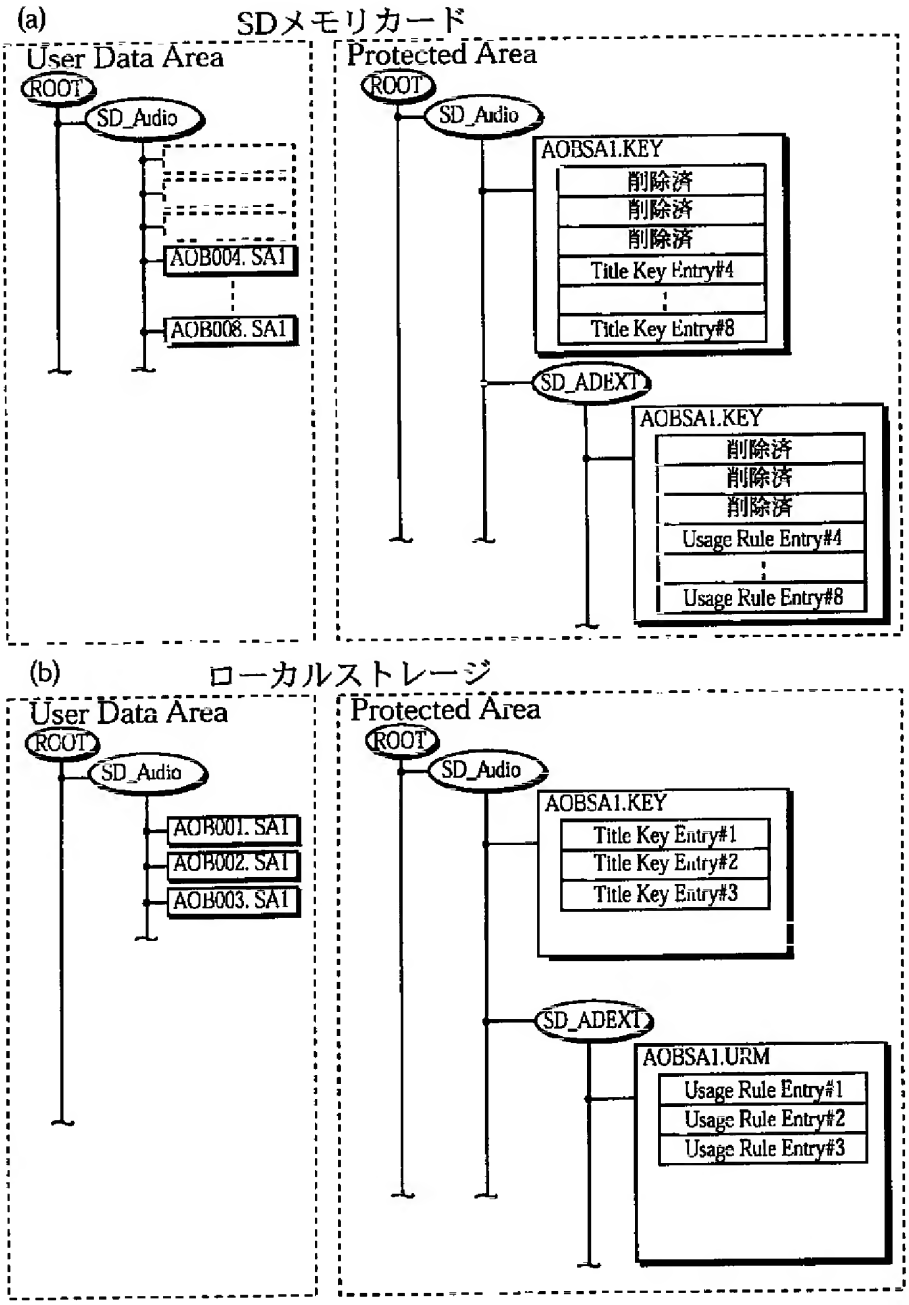
【図２８】


(a)
User Data Area
Root
SD_AUDIO
nk1
AOB001.SA1
Protected Area
Root
nk2
SD_AUDIO
AOBSA1.KEY
(b)
User Data Area
Root
SD_AUDIO
nk3
AOB001.SA1
Protected Area
Root
SD_AUDIO
SD_ADEXT
nk4
AOBSA1.URM

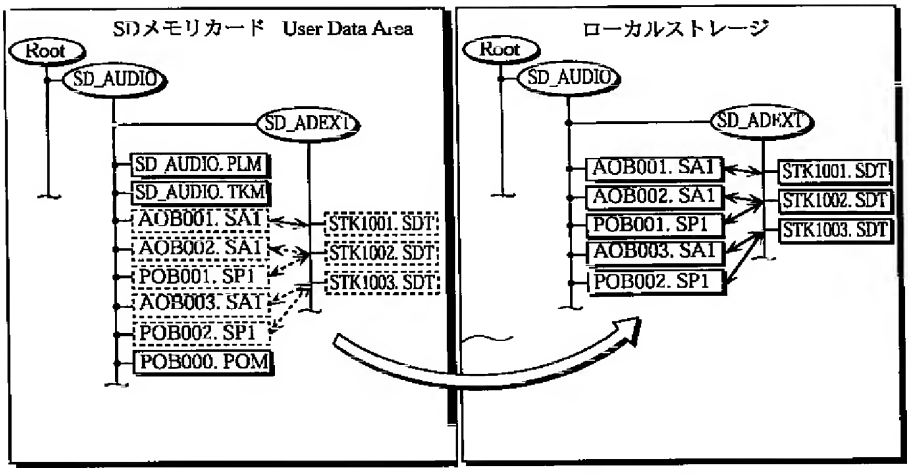
【図３０】


(a)
SDメモリカード
Root
SD_AUDIO
SD_AUDIO.PI.M
SD_AUDIO.TKM
POB000.POM
SD_ADEXT
User Data Area
MY1
MY2
MY3
ローカルストレージ
Root
SD_AUDIO
AOB***.SA1
POB***.JPG
SD_ADEXT
STK1xxx.SDT
User Data Area
(b)
Root
SD_AUDIO
SD_ADEXT
Protected Area
MY4
MY5
MY6
MY7
Root
SD_AUDIO
AOBSA1.KEY
POBSP1.KEY
SD_ADEXT
AOBSA1.URM
POBSP1.URM
Protected Area

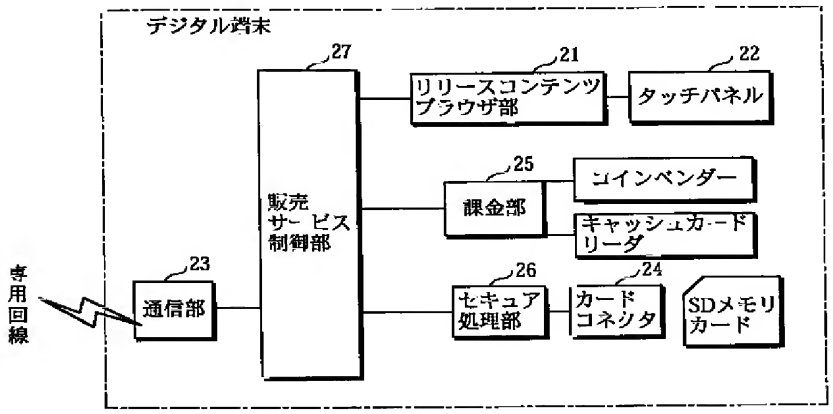
【図３１】


(a)
SDメモリカード
User Data Area
ROOT
SD_Audio
AOB004. SA1
AOB008. SA1
Protected Area
ROOT
SD_Audio
AOBSA1.KEY
削除済
削除済
削除済
Title Key Entry#4
Title Key Entry#8
SD_ADEXT
AOBSA1.KEY
削除済
削除済
削除済
Usage Rule Entry#4
Usage Rule Entry#8
(b)
ローカルストレージ
User Data Area
ROOT
SD_Audio
AOB001. SA1
AOB002. SA1
AOB003. SA1
Protected Area
ROOT
SD_Audio
AOBSA1.KEY
Title Key Entry#1
Title Key Entry#2
Title Key Entry#3
SD_ADEXT
AOBSA1.URM
Usage Rule Entry#1
Usage Rule Entry#2
Usage Rule Entry#3

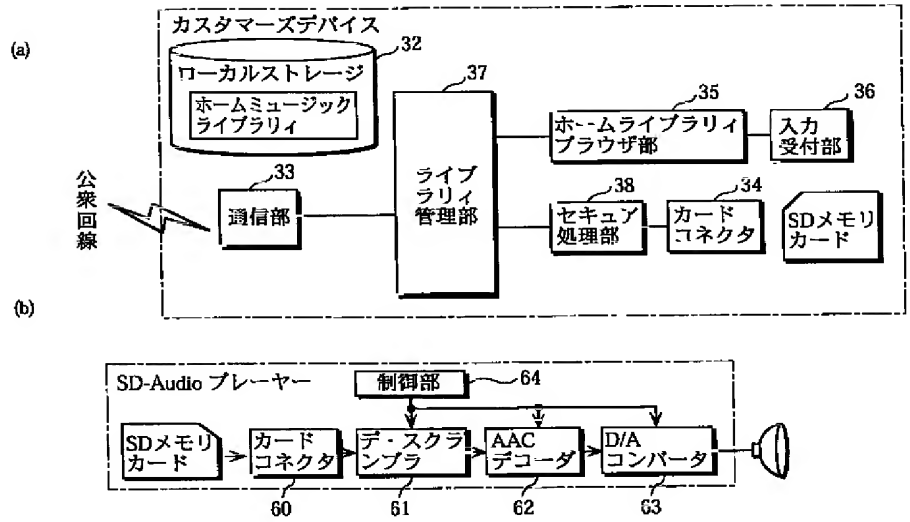
【図32】


SDメモリカード User Data Area
Root
SD_AUDIO
SD_ADEXT
SD_AUDIO.PLM
SD_AUDIO.TKM
AOB001.SA1
AOB002.SA1
POB001.SP1
AOB003.SA1
POB002.SP1
POB000.POM
STK1001.SDT
STK1002.SDT
STK1003.SDT
ローカルストレージ
Root
SD_AUDIO
SD_ADEXT
AOB001.SA1
AOB002.SA1
POB001.SP1
AOB003.SA1
POB002.SP1
STK1001.SDT
STK1002.SDT
STK1003.SDT

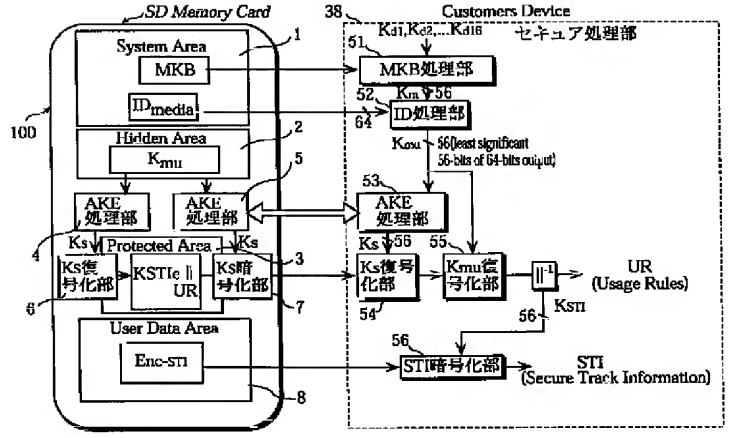
【図33】


デジタル端末
27
21
22
リリースコンテンツブラウザ部
タッチパネル
販売サービス制御部
25
課金部
コインベンダー
キャッシュカードリーダ
専用回線
23
通信部
26
セキュア処理部
24
カードコネクタ
SDメモリカード

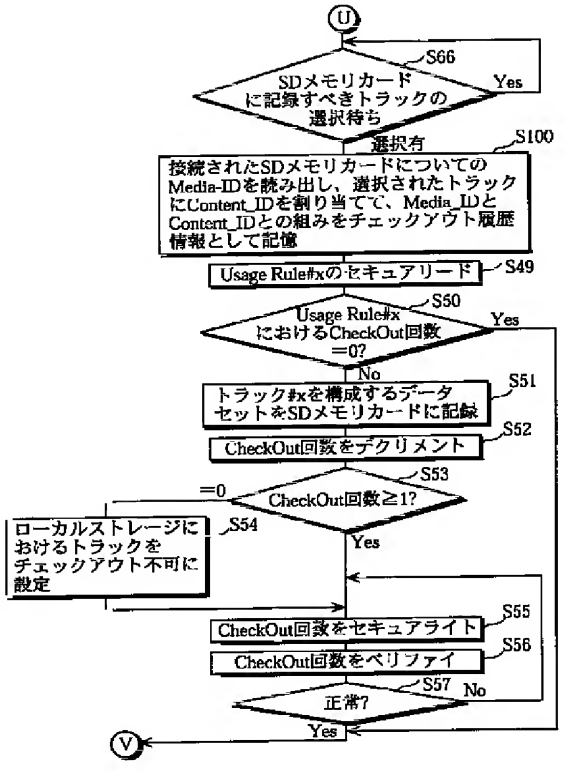
【図３４】


(a)
カスタマーズデバイス
ローカルストレージ
ホームミュージックライブラリィ
32
37
35
ホームライブラリィブラウザ部
36
入力受付部
公衆回線
33
通信部
ライブラリィ管理部
38
セキュア処理部
34
カードコネクタ
SDメモリカード
(b)
SD-Audio プレーヤー
制御部
64
SDメモリカード
カードコネクタ
デ・スクランブラ
AACデコーダ
D/Aコンバータ
60
61
62
63

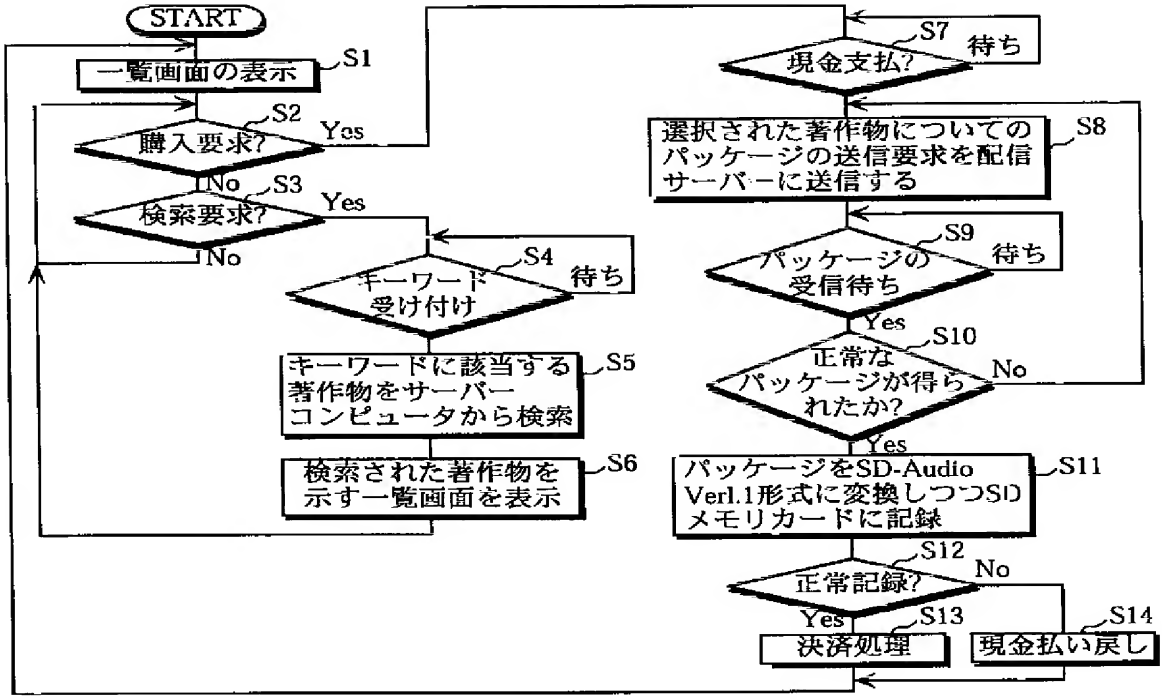
【図３６】


SD Memory Card
Customers Device
System Area
MKB
IDmedia
Hidden Area
Kmu
AKE処理部
Protected Area
Ks復号化部
KSTIe ‖ UR
Ks暗号化部
User Data Area
Enc-STI
Ka1,Ka2,...Ka16
セキュア処理部
MKB処理部
ID処理部
Kmu
56[least significant 56-bits of 64-bits output]
Ks
Ks復号化部
Kmu暗号化部
UR
(Usage Rules)
KSTI
STI暗号化部
STI
(Secure Track Information)

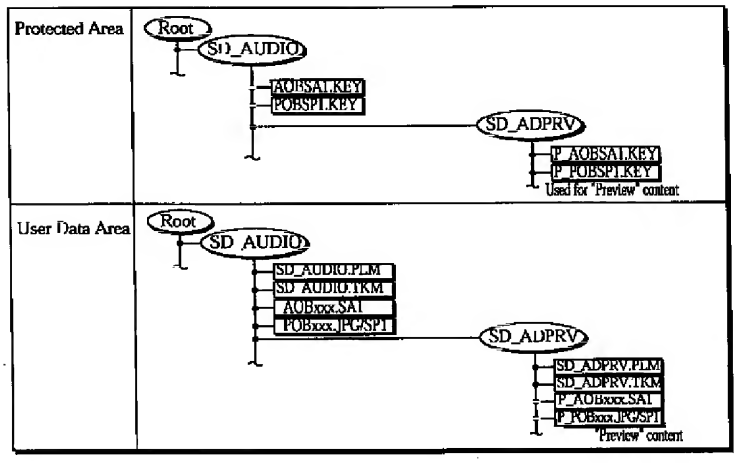
【図４０】


U
SDメモリカードに記録すべきトラックの選択待ち
S66
Yes
選択有
S100
接続されたSDメモリカードについてのMedia-IDを読み出し、選択されたトラックにContent_IDを割り当てて、Media_IDとContent_IDとの組みをチェックアウト履歴情報として記憶
Usage Rule#xのセキュアリード
S49
Usage Rule#xにおけるCheckOut回数=0?
S50
Yes
No
トラック#xを構成するデータセットをSDメモリカードに記録
S51
CheckOut回数をデクリメント
S52
CheckOut回数≧1?
S53
=0
ローカルストレージにおけるトラックをチェックアウト不可に設定
S54
Yes
CheckOut回数をセキュアライト
S55
CheckOut回数をベリファイ
S56
正常?
S57
No
Yes
V

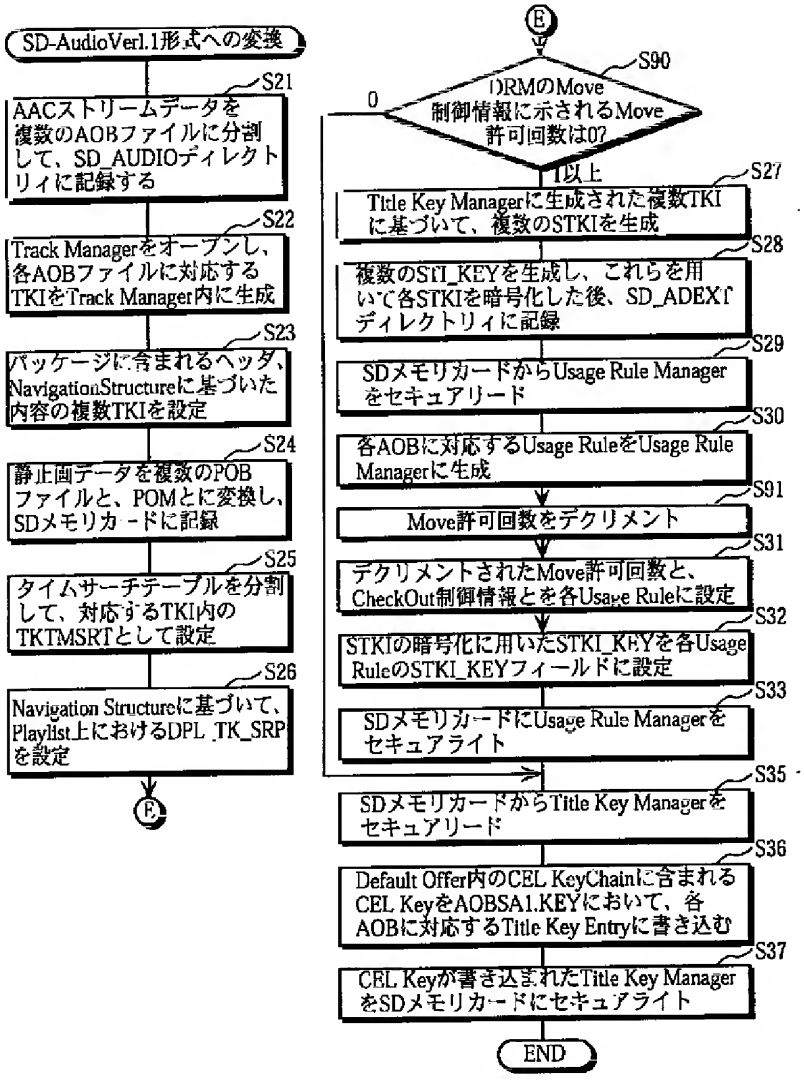
【図37】


START
一覧画面の表示
S1
購入要求?
S2
Yes
No
検索要求?
S3
Yes
No
キーワード受け付け
S4
待ち
キーワードに該当する著作物をサーバーコンピュータから検索
S5
検索された著作物を示す一覧画面を表示
S6
現金支払?
S7
待ち
選択された著作物についてのパッケージの送信要求を配信サーバーに送信する
S8
パッケージの受信待ち
S9
待ち
Yes
正常なパッケージが得られたか?
S10
No
Yes
パッケージをSD-Audio Ver1.1形式に変換しつつSDメモリカードに記録
S11
正常記録?
S12
No
Yes
決済処理
S13
現金払い戻し
S14

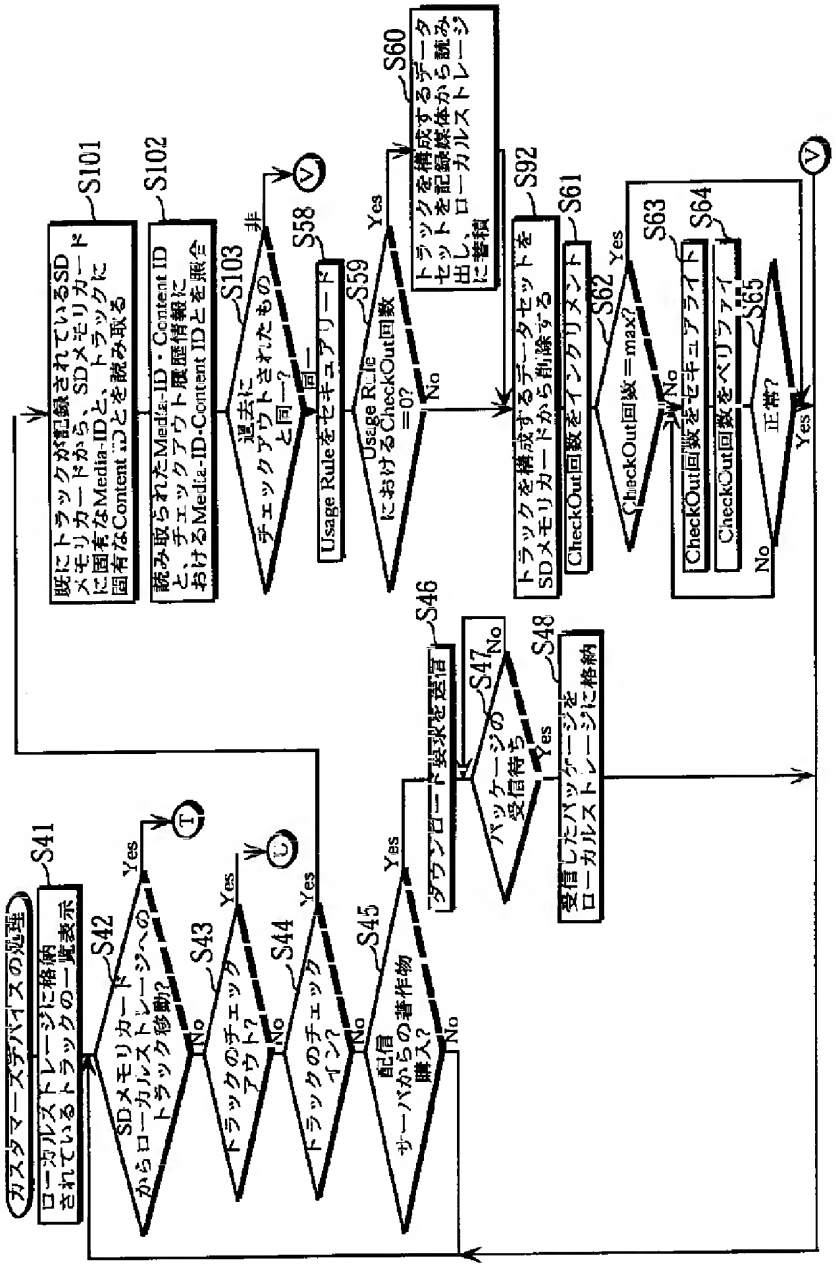
【図42】


Protected Area
Root
SD_AUDIO
AOBSAI.KEY
POBSPI.KEY
SD_ADPRV
P_AOBSAI.KEY
P_POBSPI.KEY
Used for "Preview" content
User Data Area
Root
SD_AUDIO
SD_AUDIO.PLM
SD_AUDIO.TKM
AOBxxx.SAI
POBxxx.JPG/SPI
SD_ADPRV
SD_ADPRV.PLM
SD_ADPRV.TKM
P_AOBxxx.SAI
P_POBxxx.JPG/SPI
"Preview" content

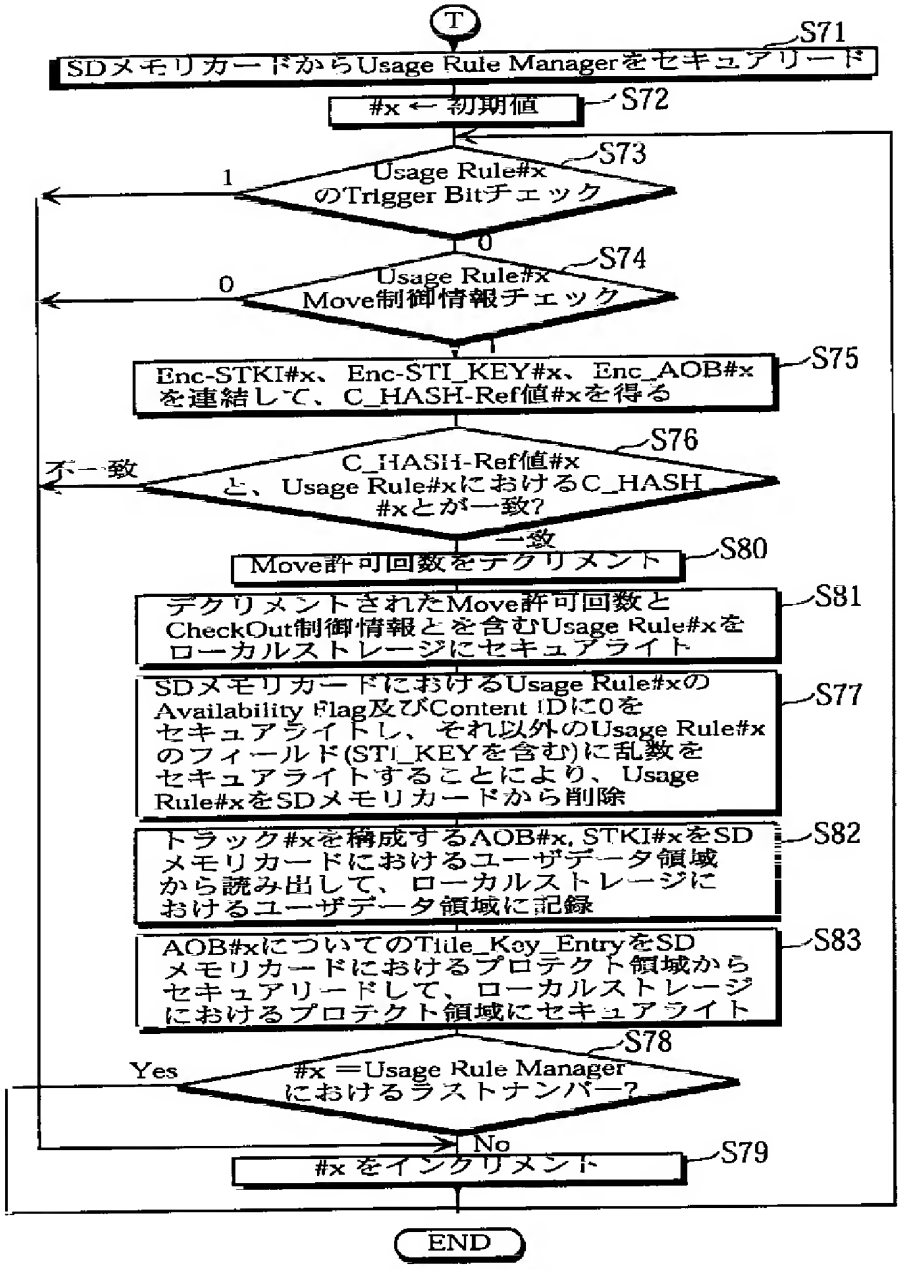
【図38】


SD-AudioVer1.1形式への変換
S21
AACストリームデータを複数のAOBファイルに分割して、SD_AUDIOディレクトリィに記録する
S22
Track Managerをオープンし、各AOBファイルに対応するTKIをTrack Manager内に生成
S23
パッケージに含まれるヘッダ、NavigationStructureに基づいた内容の複数TKIを設定
S24
静止画データを複数のPOBファイルと、POMとに変換し、SDメモリカードに記録
S25
タイムサーチテーブルを分割して、対応するTKI内のTKTMSRTとして設定
S26
Navigation Structureに基づいて、Playlist上におけるDPL_TK_SRPを設定
E
E
S90
DRMのMove制御情報に示されるMove許可回数は0?
0
1以上
S27
Title Key Managerに生成された複数TKIに基づいて、複数のSTKIを生成
S28
複数のSTI_KEYを生成し、これらを用いて各STKIを暗号化した後、SD_ADEXTディレクトリィに記録
S29
SDメモリカードからUsage Rule Managerをセキュアリード
S30
各AOBに対応するUsage RuleをUsage Rule Managerに生成
S91
Move許可回数をデクリメント
S31
デクリメントされたMove許可回数と、CheckOut制御情報とを各Usage Ruleに設定
S32
STKIの暗号化に用いたSTKI_KEYを各Usage RuleのSTKI_KEYフィールドに設定
S33
SDメモリカードにUsage Rule Managerをセキュアライト
S35
SDメモリカードからTitle Key Managerをセキュアリード
S36
Default Offer内のCEL KeyChainに含まれるCEL KeyをAOBSA1.KEYにおいて、各AOBに対応するTitle Key Entryに書き込む
S37
CEL Keyが書き込まれたTitle Key ManagerをSDメモリカードにセキュアライト
END

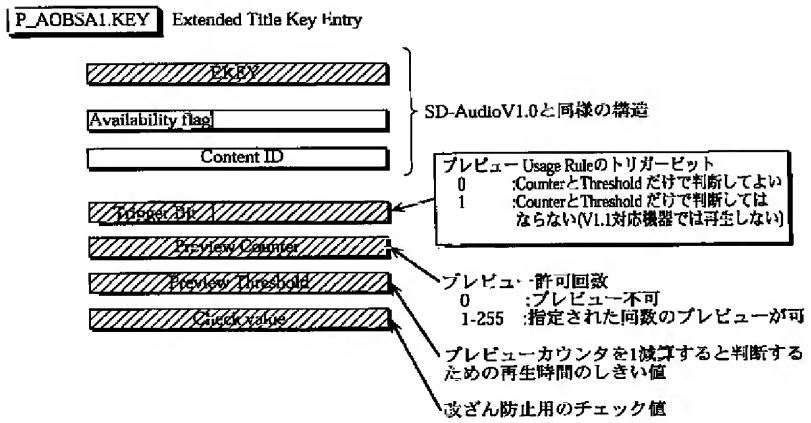
【図39】


カスタマースタデバイスの処理
ローカルストレージに格納されているトラックの一覧表示
S41
SDメモリカードのローカルストレージへのトラック移動?
S42
トラックのチェックアウト?
S43
トラックのチェックイン?
S44
配信サーバからの著作物購入?
S45
ダウンロード要求を送信
S46
パッケージの受信待ち
S47
受信したパッケージをローカルストレージに格納
S48
既にトラックが記録されているSDメモリカードから、SDメモリカードに固有なMedia-IDと、トラックに固有なContent IDとを読み取る
S101
読み取られたMedia-ID・Content IDと、チェックアウト履歴情報におけるMedia-ID-Content IDとを照合
S102
過去にチェックアウトされたものと同一?
S103
Usage Ruleをセキュアリード
S58
Usage RuleにおけるCheckOut回数=0?
S59
トラックを構成するデータセットを出し、ローカルストレージに蓄積
S60
トラックを構成するデータセットをSDメモリカードから削除する
S92
CheckOut回数をインクリメント
S61
CheckOut回数=max?
S62
CheckOut回数をセキュアライト
S63
CheckOut回数をベリファイ
S64
IE神?
S65
Yes
No
非同一
T
U
V

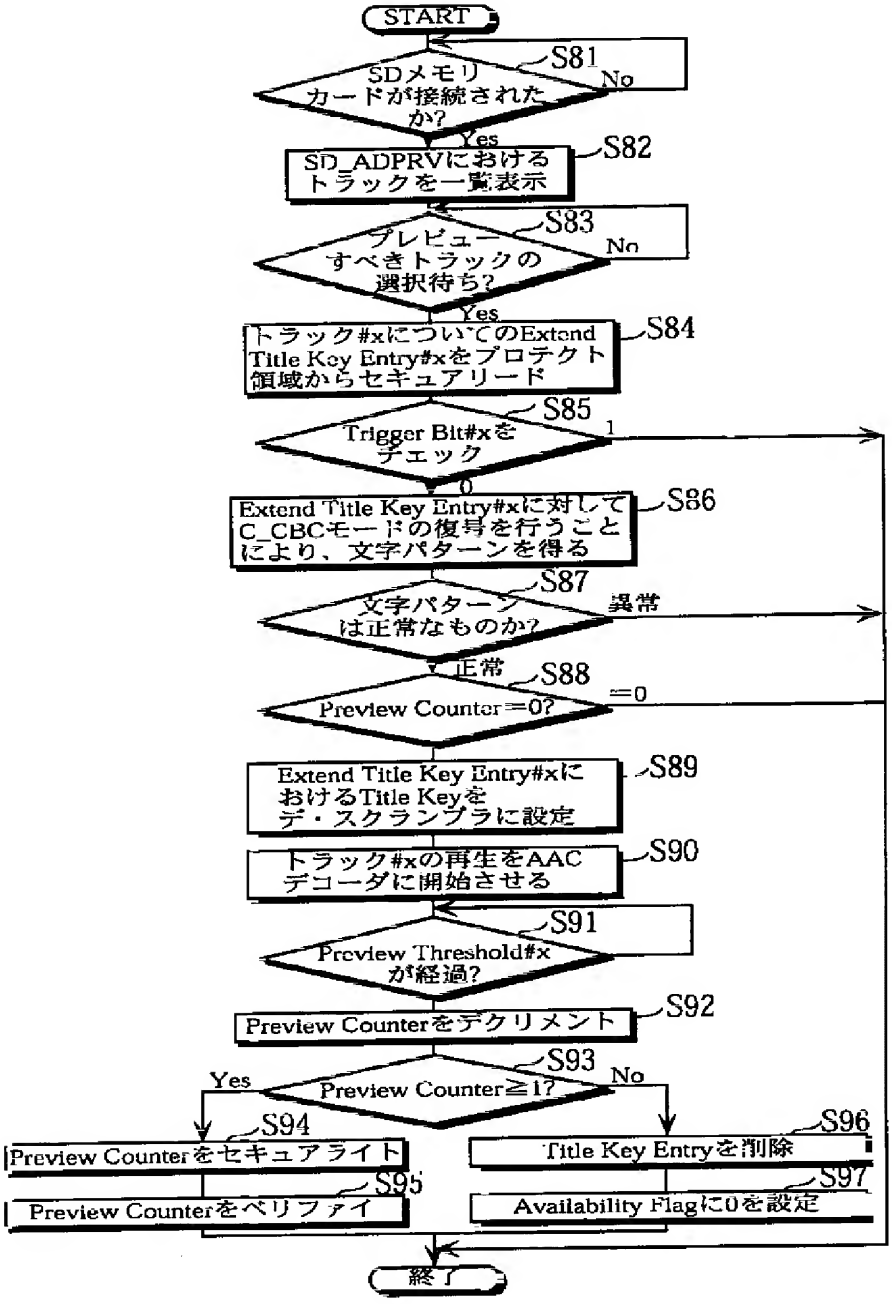
【図41】


T
S71
SDメモリカードからUsage Rule Managerをセキュアリード
#x ← 初期値
S72
S73
Usage Rule#x のTrigger Bitチェック
1
0
S74
Usage Rule#x Move制御情報チェック
0
S75
Enc-STKI#x、Enc-STI_KEY#x、Enc_AOB#x を連結して、C_HASH-Ref値#xを得る
S76
C_HASH-Ref値#x と、Usage Rule#xにおけるC_HASH #xとが一致?
不一致
一致
S80
Move許可回数をデクリメント
S81
デクリメントされたMove許可回数とCheckOut制御情報とを含むUsage Rule#xをローカルストレージにセキュアライト
S77
SDメモリカードにおけるUsage Rule#xのAvailability Flag及びContent IDに0をセキュアライトし、それ以外のUsage Rule#xのフィールド(STI_KEYを含む)に乱数をセキュアライトすることにより、Usage Rule#xをSDメモリカードから削除
S82
トラック#xを構成するAOB#x, STKI#xをSDメモリカードにおけるユーザデータ領域から読み出して、ローカルストレージにおけるユーザデータ領域に記録
S83
AOB#xについてのTitle_Key_EntryをSDメモリカードにおけるプロテクト領域からセキュアリードして、ローカルストレージにおけるプロテクト領域にセキュアライト
S78
#x ＝Usage Rule Managerにおけるラストナンバー?
Yes
No
S79
#x をインクリメント
END

【図43】


P_AOBSA1.KEY
Extended Title Key Entry
EKEY
Availability flag
Content ID
SD-AudioV1.0と同様の構造
Trigger Bit
Preview Counter
Preview Threshold
Check value
プレビュー Usage Ruleのトリガービット
0 :CounterとThresholdだけで判断してよい
1 :CounterとThresholdだけで判断してはならない(V1.1対応機器では再生しない)
プレビュー許可回数
0 :プレビュー不可
1-255 :指定された回数のプレビューが可
プレビューカウンタを1減算すると判断するための再生時間のしきい値
改ざん防止用のチェック値

【図44】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	(参考)
G06F 15/00	310	G06F 15/00	310A

(31)優先権主張番号　特願2000－125864(P2000－125864)
(32)優先日　平成12年４月26日(2000．４．26)
(33)優先権主張国　日本（ＪＰ）
(72)発明者　松島　秀樹
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　井上　光啓
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　上坂　靖
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　湯川　泰平
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　宮▲ざき▼　雅也
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　中西　正典
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　小塚　雅之
大阪府門真市大字門真1006番地　松下電器産業株式会社内
Ｆターム(参考)　5B049 AA05 BB11 CC05 CC08 DD01
DD04 EE02 EE28 FF03 FF04
FF06 FF08 GG04 GG07
5B085 AE11 AE23 AE29